Prepared Testimony

John A. Cassara

Former Intelligence Officer and Treasury Special Agent
Before the House Homeland Subcommittee on Counterterrorism and Intelligence

"Terrorist Financing since 9/11: Assessing the Evolution of al Qaeda and State Sponsors of Terror"

May 18, 2012

Chairman Meehan, Ranking Member Sanchez, and Members of the Subcommittee on Counter-terrorism and Intelligence;

Thank you for the opportunity to testify today. It is an honor for me to be here.

In 2005, I retired after a 26 year career as a Case Officer for the Central Intelligence Agency and as a Special Agent for the U.S. Department of Treasury. I believe I am the only individual to have ever been both a covert Case Officer and a Treasury Special Agent.

Much of my career with Treasury was involved with combating international money laundering and terror finance. I currently work as a contractor and consultant for a number of U.S. departments, agencies, and business enterprises, although the views that I express here are only my views and not necessarily representative of these organizations. I have been fortunate to continue my domestic and international travels primarily providing training and technical assistance in financial crimes enforcement. I have written three books on terror finance and numerous articles. I have direct experience with many of the issues being discussed here today.

A few days after the most successful terrorist attack in U.S. history, President George W. Bush stated, "Money is the lifeblood of terrorist operations. Today we are asking the world to stop payment." We are meeting here this morning in part to ask whether that request has been fulfilled and, if not, what more can and should be done.

The short answer is both "yes" and "no." Completely eradicating terror finance is impossible. There is no magic bullet. Yet after ten years of concerted effort, it is now harder, costlier, and riskier for terrorists to raise and transfer funds, both in the United States and around the world. That's the good news. Unfortunately, there is no doubt that our financial countermeasures have not been as smart or efficient as they could be and that we will continue to face new challenges in the coming years.

The learning curve has been steep. For example, in the years immediately after September 11th, most policymakers within the Treasury Department were convinced that

“financial intelligence” or Bank Secrecy Act (BSA) data was the key to following the terrorist money trail. They had misplaced faith in the approximately in (2012 numbers) 17 million pieces of financial data that are filed annually with Treasury, including approximately one million Suspicious Activity Reports (SARs). This is in addition to the countless millions of additional pieces of financial information filed around the world. This data comes from a wide variety of sources, including banks, money service businesses, and individuals.

"Financial intelligence," also known as "BSA data," or "financial transparency reporting requirements" was initiated during the early years of the “War on Drugs” when enormous amounts of illicit proceeds from the international narcotics trade regularly sloshed around western financial institutions. So it is important to understand the financial reports were not originally designed to combat terror finance where small amounts of both illicit and licit monies are commonly used. It shouldn't really be a surprise that out of the tens of millions of pieces of financial intelligence filed annually in the United States and around the world not one piece of financial intelligence was filed on any of the 19 September 11 hijackers. And even if there had been, the United States did not have the programs and management structures in place that would have detected the suspicious financial activity. I say this with confidence because I worked at Treasury's Financial Crimes Enforcement Network (FinCEN) at the time. I demonstrated the failings in my first book, *Hide & Seek: Intelligence, Law Enforcement and the Stalled War on Terror Finance* (Potomac Books, 2006). The same dearth of financial intelligence has subsequently held true for major terrorist attacks from Bali to Baghdad.

Although the last ten years have demonstrated that financial intelligence here and abroad is not the panacea for counter-terrorist finance, much of the financial data does contain excellent information and some has proved vital in "connecting the dots." The data is invaluable in money laundering and other investigations. That being said, it is not being effectively exploited.

Over the past ten years, our adversaries' operational and financial tactics have evolved. We are faced with immense challenges. The situation is made worse by the comparatively small amounts of funding involved with terror finance. For example, it is estimated that September 11 cost al Qaeda approximately $300,000 - $500,000. Even this relatively small amount towers over the recent attempt to hide explosives in a printer cartridge aboard an air cargo flight to the U.S. Al Qaeda in the Arabian Peninsula boasted in its online magazine that, “It is such a good bargain for us to spread fear amongst the enemy and keep him on his toes in exchange for a few months work and a few thousand dollars.”

While there are no simple solutions to all of the challenges identified by this subcommittee, I believe there are some straight forward and cost effective steps we should take. I have broadly categorized them as *technology, transparency, and draining the swamp.* The three are intertwined and complimentary.

Technology

Over the last few years, there have been tremendous advances in the amount of data collected and available for analysis. Just a few examples include financial, trade, transport, and travel data. Communications and social networking are growing exponentially. Industry calls these record sets of information, "big data." I will not discuss the collection of classified data.

Concurrently, there have been major advances in data mining and advanced analytical capabilities that can help organizations derive the "intelligence" from this vast amount of data. Data warehousing and retrieval are enhanced by cutting edge technologies that search, mine, analyze, link, and detect anomalies, suspicious behaviors, and related or interconnected activities and people. Fraud frameworks can be deployed to help concerned government agencies and departments detect suspicious activity using scoring engines that can both rate, with high degrees of statistical accuracy, behaviors that warrant further investigation while generating alerts when something of importance changes. Predictive analytics use elements involved in a successful case or investigation and overlays these elements on other data sets to detect previously unknown behaviors or activities, enhancing and expanding an investigator's knowledge, efforts, productivities while more effectively deploying resources. Social network analytics helps investigators detect and prevent criminal activity by going beyond individual transactions to analyze all related activities in various mediums and networks uncovering previously unknown relationships. Visual analytics is a high-performance, in-memory solution for exploring massive amounts of data very quickly. It enables users to spot patterns, identify opportunities for further analysis and convey visual results via Web reports or the iPad. Moreover, it is now possible to engineer "red flag indicators" in financial reports - both within the government and in commercial enterprises that file the information - that will identify likely suspect methodologies such a hawala or trade-based money laundering.

Unfortunately, while the federal government is beginning to incorporate these advanced analytical capabilities, it lags far behind in its deployment of commercially available and viable technologies. As a subset, the federal financial investigative resources trail even further behind. FinCEN is mandated to collect, house, analyze, and disseminate financial intelligence. FinCEN should be the U.S. government's premier financial crimes resource. However, FinCEN has never lived up to its early promise and potential. One important problem with FinCEN is that although it has attempted to implement a number of data mining activities over the years, they have not been successful. Recently, progress has been made developing and employing new analytical tools. However, the FinCEN analysts are only able to use perhaps ten per cent of their new analytical capacity. The expertise and managerial will simply do not exist to fully exploit many of the tools now finally at their disposal.

Within the next few years, it is estimated that approximately 500 - 700 million additional pieces of financial information in the form of wire transfer data will be routed annually to FinCEN. If FinCEN is not able to successfully analyze the current one million BSA filings it receives annually it is highly doubtful that it will succeed with this new tasking. Yet law enforcement and intelligence professionals should have access to the data and be

able to interpret it. Technology will be the force multiplier and the only realistic solution to effectively exploit current and new streams of financial data.

In order to move forward, we must move to get around the FinCEN impediment. I propose that we "downstream" both financial information *and* analytics platforms directly to end users in the law enforcement community. For example, the financial data *and* an accompanying user-friendly analytics platform could be made directly accessible to various task forces, U.S. attorney offices, regional Suspicious Activity Report (SAR) review teams, appropriate federal, state and local law enforcement departments and agencies. Since FinCEN is mandated by the Department of Treasury to administer the Bank Secrecy Act (BSA) and accompanying data, FinCEN could license and control the release of the data and the analytics platform.

Moreover, in my discussions with members of the U.S. intelligence and defense communities, frustration is often expressed that they do not have direct access to appropriate and targeted financial databases that intersect with their international areas of responsibility. Instead of looking for ways to increase the dissemination of necessary data, legal advisors within Treasury work to impede the release of information. While I certainly understand and endorse privacy and other concerns, the technology exists today to engineer safeguards into the dissemination of the data to prevent abuse. I urge that our colleagues be given increased access to this vital information in order to help safeguard our security.

Transparency

Shortly after the September 11 terrorist attacks, I had a conversation with a Pakistani businessman involved with the underworld of crime. He was involved in the gray markets of South Asia and the Middle East. He said, “Mr. John, don't you know that the criminals and the terrorists are moving money and transferring value right under your noses? But the West doesn't see it. Your enemies are laughing at you.”

His words infuriated me because I knew he was right. I worked overseas for years with frequent travels to the Arabian peninsula, Africa and South Asia. For the most part, U.S. officials could not understand or identify the opaque, indigenous but very effective ways of transferring money and value so different from our own. For example, the above Pakistani businessman was referring to various forms of what we loosely call “trade-based money laundering.” It involves the transfer of “value” via commodities and trade goods. In addition to customs fraud, trade-based value transfer is often used to provide “counter-valuation” or a way of balancing the books in many global underground financial systems - including some that have been used to finance terror.

In theory, by promoting trade transparency and using technology to spot anomalies in trade data (and overlapping those flagged anomalies with financial, travel, transportation, law enforcement and other databases) we may be able to use trade as a "back door" to enter into previously hidden underground financial networks.

Trade-based money laundering scams take a wide variety of forms. For example, it could be simple barter or a commodity-for-commodity exchange. In certain parts of Afghanistan and Pakistan, for example, the going rate for a kilo of heroin is a color television set. Drug warlords exchange one commodity they control (opium) for others that they desire (luxury and sports utility vehicles). In the United States and Mexico, weapons go south and drugs come north. However, generally speaking, money laundering and value transfer through simple invoice fraud and manipulation are most common. The key element here is the misrepresentation of the trade good to transfer value between importer and exporter. The quantity, quality, and description of the trade goods can be manipulated. The shipment of the actual goods and the accompanying documentation provide cover for "payment" or the transfer of money. The manipulation occurs either through over-or under-valuation, depending on the objective to be achieved. To move money out of a country, participants import goods at overvalued prices or export goods at undervalued prices. To move money into a country participants, import goods at undervalued prices or export goods at overvalued prices. For the most part, all of this avoids countries' financial intelligence reporting requirements.

Trade-based value transfer is found in every country around the world. I believe it is the "new frontier" in international money laundering and counter-terrorist finance countermeasures. Without going into detail, trade-based value transfer is found in hawala networks, most other regional "alternative remittance systems," the misuse of the Afghan Transit Trade, Iran/Dubai commercial connections, suspect international Lebanese/Hezbollah trading syndicates, non-banked lawless regimes such as Somalia, etc.

I have written extensively about trade-based money laundering. I invented the concept of trade-transparency units (TTUs), which is now part of the U.S. government National Anti-Money Laundering Strategy. I am delighted that the Department of Homeland Security's Immigration and Customs Enforcement (ICE) has adopted this concept by establishing the world's first TTU. There are approximately eight additional TTUs in the Western Hemisphere and more TTUs are planned.

In addition to being an innovative countermeasure to trade-based money laundering and value transfer, systematically cracking down on trade-fraud is a revenue enhancer for participating governments. Frankly, it is for this reason that many countries outside of the United States have expressed interest in the concept. In essence, these governments understand that they are not collecting the appropriate amount of duties on the goods because the values on the invoices are mis-stated. Finding new revenue, without actually having to raise tax rates, is an economic imperative.

TTUs are already proving to be valuable resources for our government and international partners. For example, in 2008 the United States and Mexico partnered in the creation of a TTU in Mexico City. Such efforts should be promoted and expanded. Congress can help by ensuring that the TTUs have sufficient resources to systematically examine trade fraud in the United States for reasons of both national security and to enhance our

revenue. We should also promote trade transparency overseas by building it into the US trade agenda.

Drain the Swamp

Since the end of the Cold War, there has been a dramatic decline in the number of countries that support and finance targeted acts of terrorism in order to achieve their national objectives. Today, Iran is the major "state sponsor" of terrorism. In the early days of al-Qaeda, the terrorist group received much of its financial resources from Osama bin Laden's personal family wealth, along with contributions from wealthy Saudi and other donors. Today, al-Qaeda and other jihadist groups have been forced to disperse and receive little centralized direction or funding. This is the good news.

With the decline of the above historical model - that is, groups with centralized command and control receiving most of their money from "state sponsors," evil regimes, and wealthy donors - terrorists and their supporters must increasingly rely on self-finance. In many cases, a symbiosis is developing between organized crime and terrorist organizations, and this sort of link has been observed around the world. As I detail in a book I co-authored with former Treasury official Avi Jorisch, *On the Trail of Terror Finance: What Law Enforcement and Intelligence Officers Need to Know* (Red Cell Publishing 2010) we have observed individual terrorists and terrorist groups involvement with narcotics trafficking, intellectual property rights violations or trafficking in counterfeit goods, cigarette smuggling, robberies, credit card scams, fraud, trafficking in stolen cars, kidnapping for ransom, extortion, and other serious crimes. Unfortunately, self-finance in this way is much harder to detect, track, and disrupt.

Given the above, "draining the swamp" or cracking down at home and abroad on local and transnational financial crime might eventually become one of the most effective strategies to combat terrorism. Even the U.S. military and international peacekeeping forces operating in lawless states have come to recognize that their adversaries, many with terrorist links, increasingly engage in traditional crime to help finance their activities.

For this strategy to succeed, law enforcement, intelligence, and military organizations must learn to look beyond the immediate circumstances of a given local crime. Whether they are confronted with narcotics trafficking, organized robbery, human trafficking or other activities, street cops, criminal investigators, and analysts alike must learn to ask whether these seemingly isolated acts have more sinister ties. Officials, both in the United States and overseas, must learn to "ask the next question" during the course of routine investigations: where is the money going?

Yet most law enforcement officers get caught up in the quick statistic. That is how they are recognized and rewarded. They are not interested, often times not allowed, and do not have the networks to determine if the local crime they uncovered has broader implications.

In my travels around the United States and overseas, I have observed first hand how little law enforcement groups actually know about following the money. It is particularly shocking because outside of crimes of passion, criminals and criminal organizations engage in criminal activity because of *greed; i.e., money.* For example, Karachi, Pakistan's largest city and economic hub, is heavily infiltrated by militants and terrorists making money through criminal activities such as cigarette smuggling, selling counterfeit goods, bank robbery, street robbery, kidnapping for ransom and other heinous crimes. Mr. Sharfuddin Memon, a director of a Karachi citizens' crime watch group, described the motivations behind this activity: "The world thinks this is about religion, but that's a mistake. *It's about money and power*. Faith has nothing to do with it."

I urge Congress to support effective training programs that educate law enforcement and intelligence officers on the importance of "asking the next question" and following the money trail. I also believe we should make much more concerted efforts - using various means - to work with international public media and other communications networks and brand terrorists for what they are: international thugs. They should not be allowed to glorify themselves. The last ten years have demonstrated that criminals are using *jihad* as a concept to legitimize their activities. By using publicity, transparency, and draining the swamp we will delegitimize them.

. . . . . .

As I said at the outset, our enemies are adept at exploiting the weaknesses in the US financial reporting system. Osama bin Laden once called these "cracks in the Western financial system." Their financial behavior has evolved. I also mentioned new financial threats on the horizon. Some of these include pre-paid gift and stored value cards; service-based laundering; mobile payments commonly referred to as "m-payments" or the use of cell phones to store, receive, and transmit money; digital currencies; virtual currencies in the on-line virtual world, etc. Unfortunately, time does not permit a full review. However, many of these and other financial threats and countermeasures that may merit scrutiny by this subcommittee were articulated over five years ago in the 2007 *National Money Laundering Strategy* written by the Departments of Treasury, Justice, and Homeland Security. The document was a blueprint for further action in the areas of financial crimes and threat finance. Unfortunately, in many areas, little or nothing has been done. I urge the subcommittee to review the document and ask hard questions about progress to date.

"Without money there is no terrorism." While this is a simplistic formula, our adversaries know that they need money to survive and fund their operations. They are proving adept and creative at finding new ways to access this lifeblood. I have profound respect for our intelligence and enforcement communities. The challenges they face in following illicit financial trails are immense.

I appreciate the opportunity to appear before you today and I'm happy to elaborate on my experiences and to answer any questions you may have.