



Identifying and Disrupting Funding Streams to Thwart Terrorist Financing and Organized Criminal Operations

Introduction

In order to function, thrive, and succeed, terrorist and criminal groups must have a continuous stream of funds available to them. This means they must have the capacity to raise funds, the means to launder funds, and the availability of funds to operate. A major source of funds is derived through fraud and other criminal activities. A diverse number of terrorist and criminal groups routinely exploit regional vulnerabilities in the global financial system to raise and launder funds for their nefarious purposes. By identifying terrorist and criminal organizational funding streams, disruptive and preventive measures can be developed which will diminish the ability of such organizations to operate, succeed and pose a threat to our national security and economy.

Fraud and money laundering are often the keys to terrorist and criminal organizational success or failure. They are important in the sense that they provide a source of funds and the means to access the funds as needed. In the last year, the financial services industry has better recognized the nexus between fraud and money laundering. Consequently, they have identified the need to break down silos between fraud and money laundering compliance components within their institutions in order to share information, particularly overlapping data. The ability to disrupt and prevent the funding streams for terrorist and criminal organizations is critical to our national security and economic wellbeing.

On February 12, 2009, Director of National Intelligence (DNI) Dennis Blair testified before the Senate Select Committee on Intelligence. DNI Blair advised the Intelligence Committee that the current global economic crisis was the primary near term security threat to the United States (U.S.). Some of the underlying reasons given by DNI Blair were the high levels of violent extremism caused by poverty and economic uncertainty and the threat of possible regime instability. Pakistan and Somalia are prime examples of countries experiencing such turmoil.

In assessing the cause of the current economic environment, it is evident that prominent business executives in the financial and business sectors spurred the financial crisis by causing subprime and investment frauds. It is bad enough to be consumed by greed and arrogance, but when prominent business executives cross the line and allow greed and arrogance to result in millions and billions of dollars in



fraud, they should be considered economic terrorists. When convicted for massive frauds, these executives should face the same criminal and civil penalties as other domestic and international terrorists.

This was the first time in six years that terrorism was not listed as the primary threat. However, this does not in any way diminish the terrorist threat to the U.S. In his testimony, DNI Blair specifically stated that Al Qaeda and its affiliates and allies remain dangerous and adaptive enemies. An intriguing and troubling question is, could they demonstrate their adaptability by exploiting the financial system during this economic crisis to facilitate new terrorist attacks?

Mustafa Abu al-Yazid, aka Sheikh Saeed, has widely been recognized as Al-Qaeda's Chief Financial Officer. He is currently the leader of Al-Qaeda forces in Afghanistan. In May 2007, As-Sahab Media Foundation conducted a rare television interview of Sheikh Saeed in Afghanistan. In part, the interview served as a fundraising technique. The interview underscored the organizational necessity of having funds available. In the interview Sheikh Saeed stated, "As for the needs of the jihad in Afghanistan, the first of them is financial. The mujahedeen of the Taliban number in the thousands, but they lack funds. And there are hundreds wishing to carry out martyrdom – seeking operations, but they can't find the funds to equip themselves. So funding is the mainstay of jihad."

Five Al-Qaeda members detained at the Guantanamo Bay detention center have plead guilty to planning the 9/11 terrorist attacks. These individuals referred to themselves as the 9/11 Shura (Consultive) Council. They include Khalid Sheikh Mohammed, the mastermind of the attack, his nephew Ali Abdul Aziz Ali (aka Ammar al-Baluchi), Waleed Bin Attash, Ramzi Binalshibh and Mustafa Ahmad Al Hawsawi. The five defendants collectively wrote a pleading admitting their guilt which was released on March 10, 2009. Their statements are reflective of the ongoing threat Al-Qaeda poses to the U.S. homeland. In their remarks they state, "Your intelligence apparatus, with all its abilities, human and logistical, had failed to discover our military attack plans before the blessed 11 September operation". (This included financial intelligence and demonstrated their awareness to U.S. financial reporting requirements). The pleading also stated, "We are terrorists to the bone...to us they (the charges against them) are a badge of honour, which we carry with honour." These individuals were specifically linked together through financial tracing and telephone communications. They await sentencing.

As an open society, we are vulnerable to exploitation. Terrorists and criminals are adept at identifying and exploiting systemic weaknesses. They understand the



importance of risk recognition and are effectively adaptable at both avoiding risk to themselves and exploiting societal risks. The two most significant areas of risk to terrorist and criminal organizations are communications and finance. These two areas consistently lead to the disruption and dismantlement of terrorist and criminal groups, operations and/or activities. Although terrorist and criminal groups consistently change their methods of operation and demonstrate adaptability at avoiding detection, they must communicate, and raise and spend money to function. This is where the government and private sector must individually and collectively develop and implement mechanisms to exploit the weaknesses of terrorist and criminal groups.

Regional Risks

In developing disruptive and preventive strategies to deal with terrorist and criminal funding streams, it is imperative to identify and understand geographical risks in terms of the regional risks they present, as well as the country specific risks. Three important elements must be comprehensively assessed. In addition to the geographical considerations already mentioned, cultural vulnerabilities and the level of criminal and/or terrorist threat must be examined. Factors to consider in assessing cultural vulnerabilities include bribery and corruption, (are they considered an accepted business practice); drug trafficking and money laundering; and lack of governmental transparency. In addition, it is incumbent to assess the level of criminal and/or terrorist threat posed by regions and countries.

The tri-border region where the borders of Argentina, Brazil and Paraguay intersect is an excellent example for defining regional risk. A combination of geography, rampant corruption, weak governments and an influx of investment spawned the growth of organized crime. The success of organized crime attracted militant groups, to include Hizballah and Hamas. Hizballah and Hamas use the tri-border area as a logistical and transshipment base. Criminal activities include money laundering, cargo theft, drug trafficking, gun running and other criminal endeavors.

Fraud and money laundering are interrelated. When addressing these crime problems, it is important to understand who we are dealing with and how they operate. Categorizing the players, we are dealing with:

- Individuals or groups of individuals
- Gangs
- Drug dealers, organizations or cartels



- Ethnic organized crime groups
- Terrorists or terrorist groups

Individuals or groups of individuals can make a career at committing financial frauds. They are adept at assessing and understanding the financial system. Fraudsters patiently identify systemic weaknesses to exploit and find opportunities to take advantage of systemic vulnerabilities. Many of these individuals are con artists. When dealing with such individuals, it is important to keep in mind that sophisticated fraudsters usually have an exit strategy. They realize their schemes have a limited useful life and, at some point, their fraud will be discovered. In the past, many of these fraudsters such as Robert Vesco and Mark Rich found a safe haven where they could not be extradited back to the U.S. In today's world, that is more difficult. The ability to extradite or render individuals has vastly improved. Likewise, the ability to trace and freeze illicit assets has been greatly enhanced. A new exit strategy for many of today's perpetrators may well be to launder and insulate ill gotten gains from the prospect of asset forfeiture or seizure.

Individuals or groups of individuals involved in fraud succumb to their temptations. They are driven by the fraud triangle, which consists of opportunity, incentive or pressure, and rationalization or attitude. When individuals are given ample opportunity to commit fraud, they are more likely to do so. This makes internal controls and the risk assessment process critically important. Personal integrity is also a factor. Individuals possessing a high level of integrity are less inclined to commit fraud, whereas individuals having limited integrity are more inclined to commit fraud. In establishing a fraud continuum based on opportunity and integrity, there are four combinations that place individuals at low risk, moderate risk or high risk to commit fraud. They are limited opportunity and high integrity (low risk); greater opportunity and high integrity (moderate risk); limited opportunity and lesser integrity (moderate risk); and greater opportunity and lesser integrity (high risk). In placing this in the context of fraud risk, this means 75% of individuals are at moderate to high risk for committing fraud. This is a troubling consideration, one that should heighten our awareness to the risk of fraud.

The Martin Frankel investigation represents a good case study of an international con man. Frankel gained control of a group of small insurance companies. He embezzled over \$200,000,000 from insurance companies in five states. Frankel gained opportunity by circumventing internal controls. He lived in a two mansion compound in wealthy Greenwich, Connecticut and maintained a lavish lifestyle,



which was his incentive. Frankel believed he was entitled to the money he embezzled, completing the fraud triangle. He had an exit strategy. Frankel fled from the U.S. with ample sums of money. He was ultimately arrested in Germany and extradited back to the U.S. Frankel was convicted and sentenced to a 17 year jail term. Interestingly, when he fled, Frankel tried to destroy records by burning them. Authorities found a “to do” list Frankel left behind. The number one item on the list was “launder money”.

Politically exposed persons (PEPS) are individuals who present a high risk of fraud based on their political stature and influence. They generally include current or former senior foreign figures, their immediate family and their close associates. Unscrupulous PEPs use their official positions to enrich themselves through a variety of means based on the opportunity presented by their official position. PEPs who have exploited the opportunity their position afforded include Hugo Chavez, President of Venezuela; Vladimiro Montesinos, former Minister of Intelligence in Peru; Manuel Noriega, former President of Panama; and Augusto Pinochet, former military ruler of Chile. These individuals engaged in a variety of activities to illegally enrich themselves. Illegal activities include political corruption, drug trafficking, weapons dealing, embezzlement, financial crimes and money laundering. PEPs such as Chavez have also established dangerous relationships with terrorist groups. In Chavez’s case, he has embraced Hizballah and the FARC, a Colombian terrorist organization.

Violent gangs have grown at an alarming pace. There are currently about 30,000 violent street gangs, motorcycle gangs and prison gangs operating in the U.S., consisting of approximately 800,000 members. Street gangs are the primary distributors of drugs in the U.S. Many gangs are associated with organized crime groups to include Mexican drug organizations, Asian criminal groups and Russian organized crime. Gangs are becoming more sophisticated and organized. This will present a growing money laundering threat. Gangs make money through a full range of illegal activity to include drug trafficking, robbery, theft, fraud, extortion, prostitution, gun trafficking and human smuggling.

Mexican drug cartels have emerged as the most significant organized crime threat to the U.S. They represent a narco-insurgency with a \$10,000,000,000 budget, employing 150,000 people. These are staggering numbers and demonstrate the magnitude of their organizational reach. Mexican cartels are responsible for the transportation of drugs into the U.S. and for laundering multiple millions of dollars back to Mexico and Colombia. These cartels are extremely violent and murderous.



They are responsible for significant violence along the Mexico and U.S. border region.

Colombian drug cartels have undergone a significant transformation in recent years. Mexican drug cartels have become more dominant and control access to the U.S. market. The Colombian government has exerted increasing pressure on Colombian drug cartels. Large Colombian drug organizations have become more vulnerable to detection and disruption. Hence, groups have become more fragmented. The FARC, a Colombian terrorist group, has taken advantage of the opportunity to take over functions of Colombian drug cartels. The FARC has established partnerships with corrupt Venezuelan officials and has used Venezuela as a safe haven.

The Taliban is a terrorist group. They also control the opium trade in Afghanistan, making them a drug organization as well. Between 1996 and 2001, they earned between \$30 and \$50,000,000 a year. Between 2005 and 2007 their earnings increased to \$250 and \$300,000,000 per year. The Taliban uses portions of these funds to purchase weapons and to pay for training camps. Russian gangsters purchase heroin from the Taliban. They pay with weapons and ship the heroin to Britain. The Taliban's drug trafficking operations are supported by Al-Qaeda. The Taliban operates in Afghanistan and Pakistan.

Italian organized crime has approximately 125,000 members and 250,000 affiliates worldwide. More than 3,000 members and affiliates are located in the U.S. Their criminal activities are international. In addition to Italy, members and affiliates are located in Canada, South America, Australia and Europe. They collaborate with other international organized crime groups. The major threats Italian organized crime pose to the U.S. are drug trafficking and money laundering. Other illegal activities they engage in include gambling, public corruption, extortion, kidnapping, fraud, labor racketeering, counterfeiting, infiltration of legitimate business, murder, bombings, and weapons trafficking.

Eurasian criminal enterprises are comprised of criminals born in, or with family from, the former Soviet Union or Central Europe. They operate in numerous countries around the world. Their criminal activities cause hundreds of millions of dollars in losses through sophisticated fraud schemes and public corruption. In the U.S., criminal activities include healthcare fraud, auto insurance fraud, securities and investment fraud, money laundering, drug trafficking, extortion, auto theft, interstate transportation of stolen property, human smuggling and prostitution.



Asian criminal enterprises have operated in the U.S. since the early 1990s. These groups have ties to China, Korea, Japan, Thailand, the Philippines, Cambodia, Laos and Vietnam. Asian enterprises rely on extensive networks of national and international criminal associates. They are fluid and extremely mobile. More of these criminal enterprises are engaging in white collar crimes. Asian groups co-mingle their illegal activities with legitimate business ventures. Illegal activities they engage in include racketeering, extortion, murder, kidnapping, drug trafficking, theft, money laundering, gambling, prostitution, loan sharking, human smuggling, financial fraud, and counterfeit goods.

African criminal enterprises have developed quickly since the 1980s. The political, social and economic conditions in African countries like Nigeria, Ghana, and Liberia have helped African criminal enterprises expand globally. Nigerian criminal enterprises are the most significant of these groups. Their activities in the U.S. date back to the 1970s. Nigerians operate in more than 80 countries. They are recognized globally for their financial frauds. Fraud activities of African criminal enterprises include insurance fraud involving auto accidents, healthcare fraud, life insurance fraud, bank, check and credit card fraud, advance fee schemes known as 4-1-9 letters, and document fraud to develop false identifications.

Al-Qaeda represents the most significant terrorist threat to the U.S. It was established and led by Osama Bin Laden and is a Sunni Islamic extremist organization. Al-Qaeda operates globally having a significant presence in Pakistan, Afghanistan, Iraq, Africa, and Europe. They have multiple funding sources which include front organizations, both legitimate and illegitimate; donations from like-minded supporters; charities and non-government organizations; Iran; and criminal activities. Al-Qaeda's criminal activities include drugs, fraud, kidnapping, extortion, bank robbery, human smuggling and false identification.

With the intense focus on Al-Qaeda, regional groups loosely affiliated with and easily influenced by Al-Qaeda have emerged and are located throughout the world, particularly in the Middle East, Africa, Asia and Europe. Many of these groups have been responsible for deadly terrorist attacks. Funding sources for regional Al-Qaeda related groups include Al-Qaeda, donations from likeminded supporters, charities and non-government organizations, and criminal activities. Their criminal activities include drugs, fraud, kidnapping and extortion.

Many countries, to include the U.S., Canada and the United Kingdom, are extremely concerned about homegrown cells. The diversity of homegrown extremists and the direct knowledge they have of the U.S. and vulnerabilities in the U.S. makes the



threat posed by homegrown cells serious. In the U.S. we have had the group that planned to kill soldiers at Fort Dix, New Jersey, and the group from Miami, Florida, that discussed blowing up the Sears Tower in Chicago, Illinois, and the FBI office in Miami, Florida. Homegrown cells go through a radicalization process. Fortunately, to date in the U.S., these groups have been less sophisticated and identifiable. Their funding sources have included personal income derived from legitimate jobs, criminal activity, government entitlement funds and donations.

Hizballah is a radical Shia group formed and headquartered in Lebanon. It operates a worldwide network relying on Lebanese expatriates. This extensive network has a very effective infrastructure, enabling Hizballah to operate like an organized crime family. In fact, in addition to being a terrorist organization, Hizballah is considered the best functioning organized crime family in the world. They pose a significant threat to Israel. Hizballah is primarily a fundraising threat to the U.S. However, they would be a physical threat if they thought the U.S. would take action against Iran or Hizballah or in retaliation for Israeli actions. Hizballah operates in a close knit cell structure. Their funding sources are varied. They have front companies which operate legitimate or illegitimate businesses. Hizballah uses these front companies to sell counterfeit goods and to facilitate invoicing schemes through import and export operations. As noted above, Hizballah functions like an organized crime family. They are extremely adept at conducting criminal activity. These activities include drugs, fraud, bust out schemes, extortion, and money laundering. Other sources of funds include donations from Lebanese expatriates. Hizballah also receives significant funding from terrorist state sponsors Iran and Syria. The North Carolina cigarette smuggling case "Operation Smokescreen" is an outstanding case study demonstrating how a close knit Hizballah cell raised millions of dollars through criminal activities and donations from the Lebanese expatriate community. In addition to being a fundraising cell, this group was well positioned to be an operational terrorist cell if required to be. However, their fundraising capabilities have made the chance of them becoming operational a remote possibility.

Hamas is the main Islamist movement in the Palestinian territories. They do not recognize the right of Israel to exist. Hamas is a primary terrorist threat to Israel. They are a terrorist threat to U.S. interests. Hamas operates an extensive social services network and terrorist wing. Many countries do not consider Hamas' social service network to be a terrorist organization. Rightfully, the U.S. does not distinguish between the charitable and military factions of Hamas and has designated the entire organization a terrorist organization. Hamas is masterful at using charitable fronts for fundraising and logistical support for their



military/terrorist activities. Their funding sources include Palestinian expatriates, Saudi Arabian benefactors, other Arab state benefactors, charities in North America and Western Europe, Iran, Hizballah, taxes, and extortion. The Holy Land Foundation was a Texas based Hamas charity that was shut down by the U.S. government in 2001. The charity and five principals were convicted of providing material support to Hamas in 2008. This case exemplified how Hamas used charitable fronts and also demonstrated how difficult prosecuting these types of cases can be.

Domestic terrorist groups are based and strictly operate within the U.S. The U.S. must be consistently vigilant to the threat imposed by domestic terrorism. The attack by Timothy McVeigh on the Oklahoma City federal building should serve as a constant reminder of the threat domestic terrorists. Domestic terrorists are motivated by political or social issues. They use violence and criminal activity to further their agendas. Domestic terrorist groups include white supremacists, militia/sovereign citizen movements, black separatists, animal rights extremists, and eco-terrorists. Their funding sources include personal income from legitimate jobs; business fronts, both legitimate and illegitimate; donations; criminal activities such as fraud, false identity and petty crimes; and weapons sales. An example of a domestic terrorist could be found in Gale Nettles. Nettles was convicted of counterfeiting. While serving his prison term he planned to blow up the Chicago federal building upon his release. Nettles planned to use a more powerful bomb than the one used by McVeigh in Oklahoma City. Another inmate reported Nettles. Following release from prison, Nettles purchase 2000 pounds of fertilizer from an undercover FBI agent. He paid for the fertilizer using counterfeit currency. Nettles was convicted and is serving a life prison sentence.

Global Financial Crisis

Fraud and money laundering are interconnected. The proceeds of fraud and other criminal activities need to be laundered in order to give the appearance of legitimacy. Terrorist and criminal groups must have sources of funds. Frequently such sources are derived through fraud. In order to succeed, the funds derived through fraud must be available to the organization. In order to make the funds available, the funds must be laundered.

There is an old saying, "If it seems too good to be true, it usually is." The global financial crisis was driven by greed and creative financing, and investment vehicles which were extremely risky. These risky financing and investment vehicles fell apart



causing the financial crisis and downfall of many financial institutions. As investment money became scarce, a new phenomenon emerged in late 2008, and early 2009, in the form of Ponzi schemes (investment fraud schemes). It started with the Bernard Madoff investment fraud case. Madoff ran a Ponzi scheme that resulted in a \$65,000,000,000 fraud. Next came a stream of at least ten large multi-million dollar Ponzi schemes. The fraudsters responsible for these schemes have been dubbed the mini-Madoffs. This was followed by the \$8,000,000,000 Ponzi scheme orchestrated by the Stanford Financial Group.

The economic boom preceding the financial meltdown made investors more susceptible to investment fraud schemes. They were tempted and swayed by the promise and lure of high returns on their investments. Unfortunately, they did not consider the reasonableness of the returns before investing and losing substantial sums. Schemes began to emerge in part because of the economic downturn. More people were seeking to cash in their investments. This, coupled with the lack of new investment money, meant the fraudsters could not cover their schemes and perpetuate their frauds. To succeed, Ponzi schemes must continuously bring in new investment money to cover the fraudulent outflow of funds. Another factor contributing to the discovery of these frauds was the media attention attributed to Madoff. This caused many investors to question their investment advisors and determine there were problems.

Detecting investment fraud begins with conducting adequate due diligence. Investment fraud indicators should start with the saying, "If it seems too good to be true, it usually is." If there are unusually high and consistent investment returns, due diligence should be more comprehensive. You must assess the reasonableness of the returns. The less reasonable the returns the more enhanced the due diligence should be. In both the Madoff and Stanford cases, there was a lack of transparency and a lack of oversight, where controls were circumvented. The lack of transparency and oversight resulted in select individuals having unfettered access to funds, which is conducive to fraud. In assessing Madoff, the mini-Madoff's and Stanford from the standpoint of the fraud triangle, the opportunity came from a lack of controls, incentive/pressure was caused by extravagant life style demands, and rationalization/attitude was the result of greed or a sense of entitlement.

Organized Crime and Terrorism Nexus

Organized crime groups are incorporating characteristics and methods of operation from terrorist groups. Likewise, terrorist groups are adopting strategies learned



from organized crime. This evolution makes both groups stronger, more flexible and adaptable. The tri-border region exemplifies this. Organized crime established a lucrative region to operate from. Hizballah assessed this and set up similar criminal enterprises. They were so effective that organized crime adopted some of Hizballahs methodologies to improve their efficiencies.

In comparing organized crime and terrorist groups, there are a number of organizational similarities and differences that should be considered. In terms of differences, the primary is that organized crime is motivated by profit and greed. They seek an economic end. Terrorist groups are primarily motivated by ideology. They seek a political end. From an investigative standpoint, it is easier to pursue organized crime because the greed factor is a vulnerability that can be exploited. It is more challenging to investigate terrorist groups from this perspective because ideology is extremely difficult to exploit. Organized crime and terrorist groups share a number of similarities to include corruption, violence, need for safe havens, need for recruits, a group identity and network or cell based structures. The most important similarity is that money laundering is an essential operating tool. If they are going to succeed from an organizational perspective, they must be able to launder money.

In order to disrupt the funding flows to criminal and terrorist organizations, four specific dimensions must be assessed and understood. First is the organization itself. Where does the organization operate? What are the threats posed? How does the organization raise, move and ultimately use funds? Second is funding capacity. What is the organization's source of funds? How does it launder funds? Where and how are funds made available? Third are funding mechanisms. Organizations rely on the formal banking system and informal systems. Which system, or combinations of systems are organizations inclined to use? Organizations want to avoid detection and will use a system designed to facilitate the flow of funds. Use of the formal or informal system will depend significantly on the system prevalent in the regions the organization operates in. The formal system includes financial institutions. The informal system ranges from the underground banking system known as hawala to the use of cash couriers and bulk cash shipment. Hawala is an informal and trust based system that operates parallel to the formal banking system. The fourth dimension is group members. What is the function of the individuals, and what are their funding requirements? How will they use the formal or informal financial systems?



The FBI refers to the funding cycle, especially in describing terrorist financing. The funding cycle is the organization's ability to raise, move, store and spend money. Raising and spending money go to funding capacity. Moving and storing funds go to funding mechanisms. The funding cycle for criminal and terrorist groups will be similar in many respects and different in select respects. Organizations will use the mechanisms that provide them the best opportunity to raise, move and use funds without being detected.

Money Laundering and Terrorist Financing

When assessing money laundering risks, it is important to understand who and what you are dealing with. Who is the enemy, and what is the threat they pose? In the post 9/11 world, this is an increasingly vexing question. As criminal and terrorist organizations increasingly interact and/or pattern their financial activities after each other, it becomes more challenging to answer these questions. Overall, the enemy can be categorized in two broad groups, terrorists and criminals. Terrorists are motivated by ideology and present a threat to national security. Criminals are motivated by greed, in the form of profit and/or power, and represent a threat to the economy.

What is money laundering? It is a process (financial transaction) through which income of illegal origin is intentionally concealed, disguised, or structured to avoid reporting requirements or used to promote a scheme or organizational activity. According to the International Monetary Fund and a U.S. Senate report, the estimated volume of money laundering is between two and five percent of the global gross national product, which is equivalent to approximately \$800,000,000 and \$2,000,000,000.

Money laundering is a three step process. Funds are deposited into the financial system (placement); the funds are moved to other institutions to obscure their origin (layering); and funds are used to acquire legitimate assets (integration) or in the case of terrorists, used to finance terrorist activities.

The most important distinction between criminal money laundering and terrorist financing is the overall flow of funds. For criminal purposes, the funding flow is circular. This means that the person(s) or entities responsible for laundering the funds are the direct beneficiary. The funds move in a circular pattern from the individual or entity through the system and back to the same person(s) or entities. For terrorist purposes, the funding flow is linear. The individuals responsible for laundering the money are not the direct beneficiaries of the funds. The funds flow



in a linear fashion to other members of the terrorist group, who in turn use the money to support terrorist activities. Examples of circular and linear money laundering flows involve the cases of Vladimiro Montesinos and Shawqi Omar.

Vladimero Montesinos was a PEP. He was the former Minister of Intelligence in Peru. Montesinos used his position to embezzle funds, deal in drugs and weapons trade, as well as other criminal activity. He was responsible for laundering in excess of \$400,000,000 globally, \$80,000,000 of which flowed through the U.S. The funds were laundered in a circular fashion and were intended to support and pay for safe haven for Montesinos after he fled from Peru. Until he was captured and returned to Peru, Montesinos was the direct beneficiary of the laundered funds.

Shawqi Omar was a naturalized U.S. citizen who was arrested in Iraq as a top lieutenant of Abu Musab al-Zarqawi. Zarqawi was the most feared terrorist in the world until he was killed by U.S. forces. Omar was an important lieutenant to Zarqawi because of his ability to raise money. Omar received much of his funds from family members in the U.S. The Omar family group committed multi-million dollar frauds, to include mortgage fraud. They laundered proceeds of their criminal activity through Jordan and into Iraq. The family did not benefit from the criminal proceeds sent to Jordan. The proceeds flowed in a linear fashion to Shawqi Omar in Iraq to use to support his terrorist activities.

Current and Emerging Trends

Warning signs constantly evolve due to changing dynamics and world events to include the international response to terrorism and criminal organizations. The ability of criminals, and especially terrorists, to adapt to changing dynamics to avoid detection is extremely fluid. Criminals, particularly fraudsters, and terrorists are non-static. They are adaptable and adept at changing characteristics and identifying new systemic vulnerabilities to exploit. It is incumbent that investigators monitor financial intelligence and take other steps to identify emerging trends.

The Office of Terrorism and Financial Intelligence, U.S. Treasury Department, consider cash couriers, trade based money laundering and charitable organization to be areas vulnerable to terrorist and criminal organizations. The FBI's Terrorist Financing Operations Section (TFOS) believes terrorists and criminals have reverted back to informal channels due to the increased monitoring and reporting requirements of the formal financial system. As a result, such organizations rely on cash couriers, bulk cash smuggling and the use of Hawalas. In addition, TFOS is



concerned that terrorists and criminals are taking increasing advantage of technological advancements and benefiting from the anonymity provided by virtual and internet transactions.

In assessing trends in the financial market, it should be noted that innovation drives business opportunity. Innovation also drives business vulnerability and exploitation. Innovation has resulted in the increased use of electronic transfers; increased use of technology, to include the internet and mobile devices; increased use of credit and debit cards; decreased use of checks; and the decreased use of currency. As a result, we have a changing regulatory environment.

The economic crisis has resulted in financial institutions closing or being sold, requiring the integration of legacy systems. The crisis has also resulted in significant institutional budget cuts. This has caused massive staff layoffs. The loss of talented, experienced compliance professionals is problematic. Coupled with other resource reductions, including training and monitoring capabilities, financial institutions will be at greater risk for fraud and money laundering. Fraudsters and money launderers are well aware that fewer compliance resources are being tasked to handle greater responsibilities, thereby giving the bad guys better opportunities to exploit the financial system. What financial institutions must come to terms with is Bank Secrecy Act reporting requirements have not and will not change. Therefore, financial institutions must be careful to adequately prioritize their diminished compliance capabilities.

Terrorist and criminal organizations constantly exploit systemic vulnerabilities. On October 3, 2001, I testified before the House Committee on Financial Services. I advised that vulnerabilities or high risk areas in the financial services sector at that time included wire transfers, correspondent banking, fraud and money services businesses (MSBs). The vulnerabilities as of July 13, 2009, continue to be wire transfers, correspondent banking and fraud. It should be noted that fraud is more visible in 2009 than it was in 2001. MSBs are less problematic. The more specific vulnerability than MSBs is illegal money remitters and/or hawalas. Shell companies should also be considered a current vulnerability because of their lack of transparency and ability to shield beneficial ownership.

Three case studies emphasize the five current vulnerabilities or high risk to the financial services industry mentioned above.

1. The first involves the Lloyds TSB “stripping” case. Lloyds entered into a deferred prosecution agreement with the Manhattan District Attorney and



U.S. Department of Justice and paid a \$350,000,000 fine for its fraudulent activity. Lloyds had correspondent banking relationships with Iranian and Sudanese banks. Because of U.S. Office of Foreign Assets Controls (OFAC) sanctions, Iranian and Sudanese banks were precluded from conducting business in the U.S. Lloyds Bank in London fraudulently “stripped” or removed SWIFT messaging information from incoming wire transfers from Iran and Sudan. In turn, they placed the wire transfers in their U.S. correspondent bank account. By “stripping” the SWIFT messaging instructions, they purposefully and fraudulently gave the appearance the transactions originated at Lloyds Bank in London and not in Iran or Sudan. Thus, Lloyds effectively circumvented OFAC monitoring.

2. The second case involves the Alavi Foundation. It is the successor to the Pahlavi Foundation, which was established by the former Shah of Iran as a non-profit charitable organization. The Alavi Foundation owned a 36 story office building located at 650 Fifth Avenue, an upscale location in New York City. The Alavi Foundation transferred a 40% ownership interest in the building to the Assa Corporation. The Assa Corporation was owned by Assa Company Limited a Jersey, Channel Islands shell company. Assa Corporation was wire transferring rental income to Assa Corporation Limited. Investigation determined Assa Corporation Limited was owned by Bank Melli, an Iranian Bank on the OFAC sanctions list. This meant Bank Melli could not conduct business with a company operating in the U.S. This was a violation of the International Emergency Economic Powers Act. As a result, the FBI seized the 40% ownership interest in 650 Fifth Avenue from Assa Corporation.
3. The third case involved the Carnival Ice Cream Shop, owned by Abad Elfgeeh. The shop was located in an ethnic Yemeni section of Brooklyn, New York. In addition to selling ice cream, the Carnival Ice Cream Shop operated as an illegal money remittance operation and wire transferred money for customers to Yemen and Pakistan. One of the shop’s customers was Sheik Mohammed Ali Hassan al-Moayad, an Al-Qaeda and Hamas fundraiser, who claimed to be the spiritual advisor to Osama bin Laden. Sheik Moayad was arrested in Germany in an FBI sting operation. The Carnival Ice Cream Shop had an annual income of \$185,000 yet it wire transferred \$22,000,000 overseas, mostly to Yemen. Elfgeeh was convicted of operating an illegal



money remittance business and structuring deposits to avoid reporting requirements.

The 2009 International Narcotics Control Strategy Report (INCSR), issued by the U.S. Department of State, highlights continuing vulnerabilities and potential threats to stability and security posed by global money laundering, terrorist financing and other financial crimes. According to the report, growing threats in 2009 include:

- The threat convergence of illicit drug wealth, organized crime and terrorism
- Trade based money laundering
- Service based money laundering
- Mobile payments and stored value cards laundering
- Virtual world laundering
- Suspect internet value transfer
- Growing linkage between tax evasion and money laundering

There is a nexus between drug trafficking and terrorism that is growing at light speed. The DEA linked 19 terrorist organizations to the global drug trade. DEA believes that 60% of terrorist organizations are connected to the illegal narcotics trade. As terrorist organizations become more involved in the drug trade, hybrid organizations are emerging. These organizations have morphed into one part terrorist organization and one part global drug trafficking cartel. The Taliban and FARC symbolize this transformation.

The most complex money laundering methods are often those that use trade to transfer value into or out of the U.S. Trade based money laundering encompasses a variety of schemes. They usually require under and over invoicing. The most common trade based money laundering scheme in the Western Hemisphere is the Black Market Peso Exchange (BMPE), which is operated by Colombian drug cartels.

Service based money laundering is similar to trade based money laundering. It involves service based industries such as the hospitality industry, consulting, accounting, and legal services. Fraudulent invoices and supporting documentation are used to justify payment or the transfer of money for real or fictitious services.



Service based money laundering tends to be more challenging because there is no commodity to follow.

New payment methods have evolved based on emerging technologies. These services offer convenient and valuable mechanisms. However, they are new and mostly unregulated, and therefore extremely vulnerable to criminal exploitation. Such services include stored value cards, online payment services (Paypal), digital currency (e-Gold Ltd.), mobile payments, and online virtual world transactions. The threat to exploitation is based on characteristics to include anonymous, untraceable, reusable, universally accepted, requires no intermediary, and instant settlement. Each described characteristic is extremely attractive to fraudsters. The closer an electronic payment method comes to mimicking cash, the greater the money laundering and terrorist financing threat.

Terrorists and criminals exploit the internet for a number of reasons. One significant reason is fundraising. Internet or cyberfraud ranges from credit card fraud to money laundering. Terrorists have demonstrated that they can be extremely internet savvy. Imam Samudra was the mastermind of the Bali bombing. While in prison, he wrote a jailhouse manifesto about his jihadist life. Samudra included a chapter entitled "hacking, why not", in which he detailed how to obtain credit card information through hacking. Ali Al Marri was sent to the U.S. on September 10, 2001, by Al-Qaeda, to serve as a facilitator for future terrorist attacks. He was a computer expert. When he was arrested, he had over 1000 credit card numbers and cardholder identifying information that he obtained through computer hacking. Younes Tsouli called himself Irhabi (Terrorist) 007. He committed massive cyber crimes and on line credit card fraud. Like Samudra, Tsouli posted his tradecraft on the internet for other jihadists to learn from.

Tax evasion schemes have become more prevalent and are a current criminal investigative priority for the IRS. Money laundering is the means by which criminals evade paying taxes on illegal income by concealing the source and amount of the profit. Money laundering is in effect tax evasion in progress. International business companies (IBCs) are used to facilitate tax evasion schemes. IBCs are offshore companies formed under laws of certain jurisdictions as tax-free companies. They are not permitted to engage in business within the jurisdiction incorporated in. IBCs provide confidentiality to the beneficial owner. The UBS tax evasion case exemplifies this crime problem. UBS assisted over 17,000 U.S. clients avoid and evade paying taxes on billions of dollars. Sham offshore trusts were established in Swiss banks to facilitate the UBS scheme.



Case Study

Operation Cash-Out was a wide ranging four year undercover operation. It was a multi-agency initiative led by ICE, the FBI and the IRS. It also involved local, state, and international law enforcement agencies. The level of interagency cooperation, coordination, and communication facilitated the successful results achieved in this matter. The case focused on legal and illegal money remittance businesses that were operated by ethnic Pakistanis. Due to the trust based nature of the ethnic community, these types of money remittance businesses are difficult for law enforcement to penetrate. This investigation relied on two cooperating witnesses (CWs), who acted in an undercover capacity. Based on their ethnic Pakistani background they were accepted and trusted by the subjects, and did not raise suspicion. Four separate indictments charged 45 individuals and one business in the U.S., Spain, Canada and Belgium with a variety of criminal offenses. Three indictments involved hawala and illegal money remittance businesses. Many illegal money remittance businesses function as hybrid hawalas, taking on certain characteristics of hawalas and MSBs. The CWs laundered millions of dollars through the subjects and their businesses. The CWs told the subjects the funds being laundered were drug proceeds or intended for terrorist financing. One indictment involved a scheme to bribe public officials.

U.S. v. Saifullah Ranjha, et al

Saifullah Ranjha operated Hamza, Inc., a money remitting business in Washington, D.C. Ranjha, Hamza, Inc., and five other defendants laundered over \$2,208,000 received from a CW. The money was purported to be proceeds of drug trafficking, terrorist financing and trafficking in contraband cigarettes. Through a series of hawala transactions, defendants arranged for a network of persons or businesses to transfer money to the CW's foreign bank account or to be delivered outside the U.S. Ranjha concealed the source and ownership of funds he believed were destined for Al-Qaeda. Ranjha also failed to file currency transaction reports (CTRs) in amounts ranging from \$13,000 to \$300,000.

U.S. v. Gujjar, et al

Mohammad Gujjar conspired with 24 other defendants to pay bribes to an individual they believed to be a public official of the U.S. Citizenship and Immigration Services to obtain "green cards" for themselves and their associates. Gujjar provided bribes totaling \$495,000. Gujjar and five other defendants also provided \$450,000 in



bribes to an individual they believed to be a corrupt official of the Maryland Comptroller's office to induce the release of over \$1,800,000 in Maryland sales tax assessments levied against convenience stores associated with the defendants. Gujjar was also charged with money laundering.

U.S. v. Rehman, et al

Abdul Rehman conspired with four other defendants to launder \$1,450,000 received from a CW who represented the monies were proceeds of illegal drug trafficking and the international smuggling of counterfeit cigarettes. Rahman arranged hawala transactions in the U.S. for hand to hand delivery to the CW or a designee in Spain, Australia and elsewhere. Defendants were charged with operating unlicensed money transmitting businesses.

U.S. v. Ahsan and Rehman

Mohammad Ahsan owned and operated a money remitting business in Washington, D.C., known as Pak Exchange Services. Abdul Rehman (also indicted above) conspired with Ahsan to launder \$520,000 provided by a CW, who represented that the monies were the proceeds of illegal drug trafficking. The money was given to Rehman. He used the hawala method to arrange to have the money deposited in CW's designated foreign bank account or to be delivered by Rehman and others to the CW or a designee in Canada, England, Spain, Pakistan and the Netherlands. Ahsan and Rehman were charged with money laundering. In addition, Ahsan was charged with operating an unlicensed money transmission business and failing to file CTRs ranging from \$20,000 to \$200,000.

Conclusion

Financial institutions are the gatekeepers of information about terrorist and criminal financial activity in the regulated sector. Investigations rely on bank financial data. Compliance by financial institutions with subpoenas and regulatory reporting requirements are absolutely vital. Financial records have potential value as evidence of financial crimes or questionable transactions, or to enhance other parts of an investigation. Such records include transaction records, loan applications, and signature cards. Bank Secrecy Act records, especially CTRs and suspicious activity reports are extremely valuable to law enforcement.



Financial information has both intelligence and investigative value. It can be used for strategic, tactical or historic purposes. Financial information can be used strategically for trend analysis, particularly to identify emerging trends. It can be used tactically for operational purposes to trace financial transactions in a near real time capacity. This is a proactive application. Financial information is frequently used in a historical sense to conduct traditional books and records type investigations where financial transactions are reviewed and scheduled out to develop investigative evidence. This is a reactive application. It is important to develop strategic, tactical and historic investigative methodologies to disrupt and prevent fraud and money laundering.

As noted above, there are proactive and reactive techniques available in using financial information to identify fraud and money laundering. When it comes to fraud, criminals and terrorists rely on the same methodologies. However, when it comes to using financial institutions for criminal money laundering and terrorist financing, there are vast differences. It is much easier to identify criminal money laundering than terrorist financing. It is possible to identify terrorist financing but not probable. In this regard, financial institutions and law enforcement must work closely to increase the probability and thereby improve the possibility. One step in that direction is to share information whenever possible. Disruptive and preventive measures should be paramount.

Investigators should rely on their investigative intuition and experience. They should continue to learn and broaden their investigative experience. Most importantly, investigators should ensure they stay safe. A final thought...it is a daunting task to deal with the many challenges presented by terrorist and criminal organizations. Finance and communications are the most significant vulnerabilities of terrorist and criminal organizations. It is incumbent that we continuously exploit the vulnerabilities of the bad guys and thereby, diminish their ability to function and succeed.