Fraud and Terrorist Financing

The Growing Relationship

Presented by
Maleka Ali,
Manager of Education/Consulting
Banker’s Toolbox, Inc.
There will be more attempts of terrorist activity on U.S. soil.
Fight Against Terrorist Financing is a Priority

- Low value–high volume fraud funds activities
- Partnerships with organized crime growing rapidly
- Correlation between fraud and terrorist financing and the fraud methods that are being used to finance world-wide terrorist acts
The Financing of Terror

- Not adequately understood
- Difficult to identify
- Best chance to prevent terrorists from succeeding is to disrupt their ability to raise, move, and access money
- Must have effective financial infrastructures and require financial support to achieve their goals
What If...

• Minimize the risk that your organization might be assisting terrorists in their goal of another successful attack.
• Understand the problem and determine any due diligence that you might be able to implement.
Who Is at Risk...

• All financial institutions, regardless of size, location, and product offerings are vulnerable to servicing individual criminals, groups of criminals, and criminal organizations.
• All are also equally vulnerable to facilitating terrorist financing.
Our Role...

- The role of the back office (i.e., operations, compliance, and accounting) has expanded in the fight against money laundering and terrorist financing.

- Financial Industry professionals not only play an important role in defending against the threat posed by criminal enterprises, but also play a role in safeguarding us from terrorism.
The Threats...

- An FBI assessment issued January 11, 2007, identified the following groups as threats to the United States:
  - al-Qaeda
  - Groups aligned with al-Qaeda
  - Homegrown cells
  - Shia extremists
  - Palestinian terrorist groups
  - Domestic terrorist groups
Terrorist Networks

• Terrorist network groups currently still pose the biggest security threat to the United States.
• In the immediate aftermath of 9/11, the three primary terrorist networks were:
  – al-Qaeda
  – Hezbollah
  – Hamas
al-Qaeda

- Former leader, Osama bin Laden
  - Did not come from the military
  - Was not a religious figure
  - Or a spokesperson of the poor and oppressed

- Rich man who built al-Qaeda’s financial system from a network originally designed to provide resources to the mujahedeen fighting the Russians in Afghanistan
Osama bin Laden

5/1/2011 Osama bin Laden killed in targeted attack

One of the most significant counterterrorism operations in United States history since bin Laden became the face of terrorism
Mountains of Information Recovered

- Documents recovered included:
  - Five computers
  - Ten hard drives
  - Over 100 storage documents

- Multi-agency task force reviewed and helped in the prompt warnings of plots against trains and other targets

- Triggered operations overseas, including arrests of suspects that were named or described in emails to bin Laden found on the computers
Files Revealed:

- Files described an organization weighed down by mounting financial hardships
- Suggested using kidnapping as a fundraising tool
- Showed that bin Laden was directly involved in managing the finances for the organization
- Also highlighted his obsession of attacking the United States and assassinating President Obama
Teaching Fraud

- al-Qaeda also uses the Internet as a:
  - tool for online recruiting
  - tool for communication
  - means of using fraud (and teaching how to use fraud) to raise money for their activities

- *Inspire* is an English-language Internet magazine published by al-Qaeda that provides guidance in detail for planning and implementing terrorist attacks.
Inspire—Open Source Jihad

Open Source Jihad

A resource manual for those who loathe the tyrants; includes bomb making techniques, security measures, guerrilla tactics, weapons training and all other jihād related activities.

- A disaster for the repressive imperialistic nations: *The open source jihād is America’s worst nightmare.*
- It allows Muslims to train at home instead of risking a dangerous travel abroad: *Look no further, the open source jihād is now at hands reach.*
Fourth issue, Anwar al-Awlaki, encouraged his followers to fund more attacks through crime by stealing from non-Muslims to fund their activity.

Both al-Awlaki and editor Samir Khan were killed in a drone missile attack on September 30, 2011.
Threat Not Over...

- al-Qaeda network has been disrupted, but it hasn’t been destroyed.
- As long as terrorists retain access to a financial network, they remain a threat to the United States.

Since 9/11, threats from other areas have also become more evident.

Threats expand to include regional terrorist groups, domestic terrorist groups, homegrown cells, and lone-wolf threats.
Organized Crime and Terrorist Financing

• Funding for terrorism comes from:
  – Monetary support from wealthy individuals or groups
  – Charities
  – Fraud
  – Terrorist-organized crime connection
Organized Crime Partnership

• Partnership and links between organized crime and terrorism continues to grow.

• DEA linked 19 terrorist organizations to global drug trade, and believes up to 60 percent of terrorist organizations are also connected to illegal narcotics trade.

• As terrorist organizations become more involved in drug trade, hybrid organizations are emerging.
Partners in Crime

• 12/16/09: Three al-Qaeda members were arrested in Ghana as part of a DEA investigation

• Charged with conspiracy to commit acts of narco-terrorism and conspiracy to provide material support to a foreign terrorist organization

• Between 9/09 and 12/09, al-Qaeda conspired to assist drug dealers in transporting hundreds of kilograms of cocaine from West Africa through North Africa into Spain.

• al-Qaeda agreed to protect drug shipments.
Evolution

- Organized crime groups are incorporating characteristics and methods of operations from terrorist groups.
- Terrorist groups are adopting strategies learned from organized crime.

- This evolution makes both groups stronger, more flexible, and more dangerous.
## Comparison

<table>
<thead>
<tr>
<th></th>
<th>Organized Crime</th>
<th>Terrorism</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Motivation</strong></td>
<td>Profit or greed</td>
<td>Idealism</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>Seek economic ends</td>
<td>Seek political ends</td>
</tr>
<tr>
<td><strong>Engage in Corruption</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Structure</strong></td>
<td>May be network and cell based</td>
<td>May be network and cell based</td>
</tr>
<tr>
<td><strong>Geographies</strong></td>
<td>Require safe havens</td>
<td>Require safe havens</td>
</tr>
<tr>
<td><strong>Membership</strong></td>
<td>Needs to recruit new members</td>
<td>Needs to recruit new members</td>
</tr>
<tr>
<td><strong>Specialists</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Group Identity</strong></td>
<td>Important</td>
<td>Important</td>
</tr>
<tr>
<td><strong>Threat of Violence</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Target Selection</strong></td>
<td>Select targets that pose a threat to the group</td>
<td>Select symbolic targets</td>
</tr>
<tr>
<td><strong>Publicity</strong></td>
<td>Avoid public attention</td>
<td>Seek public attention</td>
</tr>
<tr>
<td><strong>Use Money Laundering as Essential Operating Tool</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Funding

In order to understand how financial institutions fit into the overall scheme of a terrorist plot, it is important to understand the:

- Funding capacity
- Funding mechanism
- Funding cycle
Funding Capacity

• Includes source and availability of funds
• Need to raise funds necessary to accomplish their goal
• Need to have a means to launder that money, so they will have to effectively place and store that money in our financial systems

• Funds then need to be available when they need them so that they can move the funds to where they need to be to support the various terrorist cells and to fund operations
Funding Mechanism

• Includes a formal or an informal financial system.
• Formal includes our network of banks, other financial institutions, and money service businesses.
• Terrorists are drawn to jurisdictions that have inadequate or limited bank supervision, anti-money laundering laws, and/or ineffective law enforcement, especially those with lots of bank privacy.
• Informal systems include charities and hawalas.
Charities

- Charities have been an important source of funds for terrorists.
- Some of those whose donations go to terrorism know what the money will be used for; however, many others thought their money would help legitimate charitable organizations.
Hawala

• Very old, underground banking system that allows money transfer without actual money movement or any wire transfer

• Nothing essentially illegitimate about the hawala system

• Offers needed financial services in many remote corners of the globe
Hawala: How It Works

- Customer gives local *hawaladar* money.
- Hawaladar calls his counterpart across the world, who distributes money out of his own funds to the intended recipient.
- Hawaladars keep track among themselves, but because of the volume of transactions flowing through the system in both directions, the two hawaladars rarely have to worry about settlement.
- Trust between and among hawaladars, who in many cases are related through family, clan, or ethnic associates, allows them to carry each other’s debts for long periods before finding a way to clear them.
Funding Cycle

– Continuous Cycle
  • Raise the money
  • Move the money
  • Store the money
  • Spend the money

• Interrupt any of the processes within the cycle and we stand a good chance of shutting down the plot as well.
• We will concentrate below on moving and raising the money using criminal/fraudulent activities.
MOVING THE MONEY
Moving the Money

Terrorists use drug-trafficking money laundering practices to move their funds that are more common among criminal organizations such as:

- Cash smuggling
- Black market peso exchange
- Trade-based money laundering
Smuggling

• One of the oldest methods of moving money
• Cash smuggling or transfer assets into the form of precious metals and gemstones or prepaid access cards
• Easy/anonymouse
• Transfer across borders and then transfer back to cash across the globe
Smuggling Red Flags

- Exchange small bills for large
  - Not common practice for small business
- Business who should deal in check or wire requesting large amounts of cash
- Gets agitated by delays in getting large amounts of cash
- Doesn’t want cash counted (in a hurry)
- Withdrawals from many/distant branches
- Customer wants old bills
## Weight of $1 Million

<table>
<thead>
<tr>
<th>Denomination</th>
<th>Pounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1</td>
<td>2,000</td>
</tr>
<tr>
<td>$5</td>
<td>400</td>
</tr>
<tr>
<td>$10</td>
<td>200</td>
</tr>
<tr>
<td>$20</td>
<td>100</td>
</tr>
<tr>
<td>$50</td>
<td>40</td>
</tr>
<tr>
<td>$100</td>
<td>20</td>
</tr>
</tbody>
</table>
Black Market Peso Exchange

• Complex
• Began in Colombia
• Need to understand the parties involved
  – How they interact with each other and
  – How and why the exchange process began
Black Market Peso Exchange

• Drug sales in United States generate enormous amounts of U.S. dollars.
• Colombian drug cartels needed pesos in Colombia, not U.S. dollars.
• Needed to physically move the money back to Colombia and exchange dollars for pesos.
• During the 1980s, crooks simply deposited the cash into U.S. banks and wire-transferred money to Colombia.
• As U.S. investigators began to tighten controls within banks, drug traffickers had to find other ways to move the money.
• So, drug cartels turned to the peso brokers.
Peso Broker

• Informal bankers used for years to get around government currency restrictions and import tariffs
• Colombian businessmen who needed dollars turn to a peso broker
  – offered U.S. dollars
  – never asked for importation documents
• Goods could be smuggled into Colombia, avoiding heavy import tariffs
Peso Broker

- Drug cartels funneled huge amounts of U.S. dollars into the United States to these peso brokers, who in turn would sell them to Colombian businessmen.
- Brokers sent the dollars on behalf of the Columbian businessmen directly to pay for American goods.
- After goods were sold for pesos in Colombia, the Colombian businessmen could pay the peso broker back for those dollars.
- Peso broker would take a heavy cut and transfer the rest of the pesos to the drug cartels.
Black Market Peso Scheme

NARCO TRAFFICKER

DOLLARS

GOODS

PESOS

COLOMBIAN BUSINESS
Black Market Peso Exchange Signs

• Payment made in cash by a third party who has no connection to the underlying transaction involving a legitimate foreign commercial transaction

• Payment made by wire transfers from third parties not connected to the underlying transaction

• Payment made with checks, bank drafts, or money orders not drawn on the account of the purchaser of the goods in a foreign country
Broker–Terrorist–Crime Organizations

• Broker will put an organization/individual with cash offshore in contact with a local who needs hard currency.

• Group will put the money up for the local contact that, broker in turn, will make sure is made available to the gangsters in his country.

• Terrorist does not get involved in transferring the money into a different jurisdiction, does not register the exchange in the third country, and reduces the risk of being spotted by investigators.
Trade-Based Money Laundering

“Process of disguising proceeds of crime and moving value through the use of trade transactions to legitimize their illicit origins.”

TF Money Laundering Typologies

- False documentation which misrepresents the contents and/or volume of cargo
- Multiple invoicing
- Fabricating shipments
- Fresh-air invoicing (falsifying trade weights by overstating or understating quantity)
TF Money Laundering Typologies

- MONEY MOVED OUT OF THE UNITED STATES
  - Undervalued exports
  - Overvalued imports

- MONEY MOVED INTO THE UNITED STATES
  - Overvalued exports
  - Undervalued Imports
Move $50,000 from U.S. to Foreign Firm Through U.S. Export at Low Price

1. U.S. firm has $50,000 to move to foreign firm
2. U.S. firm buys 50 gold watches at $1,000 each (pays $50,000)
3. Sell/export 50 watches to foreign firm at $5 each
4. Foreign firm sells 50 gold watches at $1,000 each = $50,000
OVER-INVOICED IMPORTS

Move $50,000 from U.S. to Foreign Firm Through U.S. Import at High Price

1. U.S. firm has $50,000 to move to foreign firm
2. Foreign firm buys 10,000 pencils at $.05 each ($500) locally
3. Foreign firm sells 10,000 pencils to U.S. firm at $5 each
4. U.S. firm pays $50,000 to foreign firm
Trade Finance Red Flags

• Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.
• Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped.
• Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity’s fair market value.
• The size of the shipment appears inconsistent with the scale of the exporter or importer’s regular business activities.
Trade Finance Red Flags

• The type of commodity being shipped is designated as “high risk” for money laundering activities. For example, high-value, low-volume goods (e.g., consumer electronics), which have high turnover rates and present valuation difficulties

• The transaction involves receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction

• Changes to a Letter of Credit beneficiary just before payment is to be made

• Changes in the Letter of Credit regarding place of payment to an account in a country other than the beneficiary’s stated location
When Monitoring for Trade-Based Money Laundering

• Consider import/export companies high risk
• Perform due diligence on Letter of Credit transactions
  – Does activity make sense for business?
  – Does product described on invoice make sense for business?
  – Does amount on invoice make sense?
Raising the Money
Terrorists use many criminal fraudulent activities to raise funds and spread terror.

Bribery and corruption are accepted business practices.

Criminal/fraudulent methods used include:
- basic fraud
- drug trafficking
- human trafficking/smuggling
- counterfeit goods/currency
- stolen goods
- violent crimes
- kidnapping
- extortion
- cyber fraud
- money laundering
Raising the Money

• Tools include:
  - Internet
  - credit/debit cards
  - prepaid cards
  - illegal money remitters
  - informal transfer systems
  - shell companies
  - offshore havens
  - wire transfers
  - other electronic payment mechanisms
Raising the Money

• New payment services emerging in response to market demand have become favorite payment vehicles for online fraudsters and terrorists.
• Payment mechanisms include: online payment services, prepaid cards (i.e., credit/debit cards, gift cards, phone cards), mobile payments, online virtual world transactions, and digital currency exchange providers and dealers.
• Might be transferred to/from unknown third party, avoid border restrictions, and as transactions become mobile, might be instantaneous.
Prepaid Cards

• Prepaid cards may be loaded with money.
  – Some are reloadable and can be easily transported to another place for money laundering, bulk cash smuggling, or even to support terrorism.

• Wallets are generally not checked for prepaid cards when moving across borders, so they become an easy method to bring money across an international border without detection.
Prepaid Cards and Terrorists

• If a terrorist cell wants to carry out an attack in the United States, a credit card obtained in Europe might be handed to another cell member traveling to the United States to execute an attack.
• Bringing a wad of cash into the country would violate cash reporting laws, but there is nothing illegal about carrying cards. (new law proposed)
• Cards can even be mailed internationally.
• Terrorists link cards to mobile phones, then wire money over a wireless network to fellow cell members in another country.
Terrorists Adapt and Are Tech Savvy

- Terrorists have learned to use and manipulate the Internet and will use it to their advantage in areas from credit card fraud to raise funds, to money laundering to move and store funds.
- Imam Samudra, the mastermind behind the Bali bombing, wrote a document while in prison encouraging the use of hacking to steal money electronically.
- Ali Al Marri, an al-Qaeda facilitator for post 9/11 activity in the United States, was an expert at exploiting the Internet for fraud.
- Younes Tsouli, a/k/a Irhabi, used email and radical websites for propaganda and communications, and used the Internet for cyber crime and credit card fraud.
Stuart Levy, former Under Secretary for Terrorism and Financial Intelligence, Treasury Department, said:

“They [crooks and terrorists] are intelligent people, and they are going to be innovative, but it requires us to be innovative as well, because we now have to adjust our actions on all levels—law enforcement, regulation, and education in the private sector—to stay one step ahead.”
Actual Cases: Example One

• 2005: Stolen credit cards were used in plot to blow up the Melbourne Cricket Grounds during the Australian Football League Grand Final.
• 2008: 12 men went on trial for plotting the act.
• Plane tickets and mobile phones for the suspects were bought using stolen credit card data.
• They bought stolen card info. from taxi drivers for $10 each.
Actual Cases: Example Two

“Cyber Jihadis in UK used the Internet to urge Muslims to wage holy war on non-believers 2007: Tariq al-Daour, Younis Tsouli, and Waseem Mughal found guilty of incitement to commit terrorism Used credit card info. stolen from phishing attacks and laundered through online gambling sites to finance website promoting martyrdom through terrorist violence Stolen credit card info. was put on black market, which the terrorist cell used to establish a network of websites that enable communication among terrorists Website provided info. on topics such as computer hacking and bomb-making, and hosted videos of beheadings and suicide bombings in Iraq
Actual Cases: Example Three

- Somali native, Nuradin Abdi, was part of plot planning to blow up a Columbus, Ohio, shopping mall along with other al-Qaeda operatives
- Attended a guerilla training camp in Ethiopia
- Provided stolen credit card numbers to a man accused of buying gear for al-Qaeda
- Abdi collected the credit card numbers through his cell phone business
- Card info. was then used by an acquaintance that was in the process of buying a laptop, GPS watch, laser range finder, and other equipment for use in the terrorist plot
Actual Cases: Example Four

- Lebanese Canadian Bank (LCB) based in Beirut, Lebanon, and Montreal, accused of facilitating money laundering activities for the Joumaa organization, an international narcotics trafficking and money laundering network.
- Joumaa organization: On January 26, 2011, Ayman Joumaa, along with nine others and 19 entities attached to his drug trafficking and money laundering activities, were designated as Special Designated Narcotics Traffickers (SDNTs) by OFAC.
- On February 11, 2011, LCB was designated by the U.S. Treasury Department as an entity of primary money laundering concern.
- LCB was used by the Joumaa organization to move hundreds of millions of dollars monthly in cash proceeds from drug sales into the financial system.
- Hezbollah received financial support from the criminal activities of the Joumaa organization.
- Managers from LCB were linked back to Hezbollah.
1. Cocaine shipped from Colombia and Panama to Europe and the Mideast via Africa
2. Money from the drug sales goes to Lebanon
3. Funds are moved to U.S. based accounts to purchase used cars from American dealerships
4. Used cars are shipped to Benin and Congo in Africa
5. Money from the sales of cars goes back to Lebanon
Mitigation and Investigations
Mitigation and Investigative Tools

• Prepaid card monitoring and mitigation:
  – Collect purchaser Information.
  – Monitor all large purchases.
  – Aggregate by purchaser.
  – Track all purchases in cash.
  – Aggregate cash purchases by same purchaser.
  – Aggregate and review buyers with a high volume of purchasers.
  – Determine whether the volumes make sense.
Mitigation and Investigative Tools

• ACH Monitoring and Risk Mitigation:
  – Identify and monitor the ACH transactions of all high-risk customers.
  – Identify customers with frequent and large ACH transactions.
  – Increase your due diligence for international ACH transactions.
  – Identify and ACH transactions that the bank originates to foreign financial institutions, particularly to high-risk geographic locations.
  – Run volume reports to identify customers with unusual or large volumes of ACH or ATM activity, and ensure that ACH transactions (i.e., amounts, frequency, origin, or destination) are consistent with nature of business or occupation of customer.
Mitigation and Investigative Tools

• ACH Monitoring and Risk Mitigation:
  – Scan institutions’ transactions for *keywords* that might indicate activity that warrants higher due diligence, such as PayPal, global pay, e-gold, gambling, dirham, goldxcash, click2exchange, or other online service providers.
  – Review velocity reports to identify accounts with high turn-around transactions of cash, ACH, or ATM transactions.
    • Terrorists might transfer money via ACH and then immediately remove in cash.
    • Does the volume of this activity make sense for your customer?
  – Review spike reports to identify accounts with unusual spikes in their account activity.
Role of Financial Services

- The financial services industry has access to financial intelligence that is critical in helping law enforcement fight terrorist financing.
- Be prompt and detailed when reporting suspicious activity so law enforcement has time and the information necessary to track down terrorists before they are successful in carrying out their plans.
The key to being prompt is to understand how innovated the terrorists are being in raising and moving their money so that we can implement targeted monitoring for suspicious activity.
Proactive v. Reactive

• Need to be proactive instead reactive.
• Financial institutions and auditors need to set internal controls to identify fraud that might also be financing terrorist plots.
• Rely on your investigative/analytical intuition and experience to provide financial intelligence to law enforcement that is detailed and prompt.
• Law enforcement can use the suspicious activity reports filed by institutions to perform trend analysis and tie into possible terrorism cases.
By following the money, we can target the crooks and money launderers in order to catch the terrorists before...
Thank You

Maleka Ali, CAMS
Manager/Education & Consulting
Banker’s Toolbox, Inc.

Http://www.Bankerstoolbox.com