



## Newsletter Article

March, 2016

# HOW TERRORIST TRENDS EVOLVE AND HOW FINANCIAL INSTITUTIONS SHOULD RESPOND

By Dennis Lormel

### ABOUT THE AUTHOR

**Dennis Lormel** is President of DML Associates and a recognized subject matter expert in the anti-money laundering, terrorist financing, and fraud communities. He spent 30+ years in Government Service, Law Enforcement and the FBI. After the tragedy of 9/11, Mr. Lormel realized that the terrorists needed a financial infrastructure to accomplish the attacks. He immediately established an investigative organization within the FBI that, within days, identified the funding stream that supported these attacks.

Email: [DLormel@DMLAssociates.com](mailto:DLormel@DMLAssociates.com)

*As we move into and through 2016, the most significant terrorist threats to Western society are posed by Islamic terrorist or jihadist organizations. As evidenced by the attacks in Paris on November 13, 2015, the subsequent disruption of imminent attacks in Europe, in the aftermath of Paris, in November and December 2015, the San Bernardino attack on December 2, 2015, the attack on a police officer in Philadelphia on January 7, 2016, the suicide bombing in Istanbul on January 12, 2016, the attack in Jakarta on January 14, 2016, and the most recent bombings in Brussels this week, these events have become all too frequent. Among other issues, this article will address two questions: How did such threats emerge, and how should financial institutions respond?*

### Also at BankersHub

- April 5 – [Garnishments, Subpoenas, Summons and Levies](#)
- April 7 – [Business Account Signature Cards and Resolutions](#)
- April 8 – [Social Engineering: All About Phishing](#)
- April 11 – [ERM Enterprise Risk Management: Making It Work](#)
- April 13 – [Wire Fraud Risk Exposure that You May Be Overlooking](#)
- April 14 – [Compliance in Commercial Lending: Understanding Key Regulations](#)
- April 14/15 – [Loan Structuring Basics](#)
- April 18 – [Getting Ready for Proposed FFIEC Call Report Changes](#)
- April 19 – [Consumer Complaint and Response Management](#)

### Emergence of Terrorist Trends

Developments in terrorism are driven by numerous factors. These factors can be categorized as being either inherent or adaptive. Inherent factors are primarily driven by ideology and politics. With respect to Islamic terrorism, ideology is driven by the desire to establish a global caliphate or state. Politics is predominantly centered upon Sunni versus Shiite dynamics and conflict. The Sunni and Shia conflict dates back to the year 632, following the death of the Prophet Muhammad. The Sunni – Shia split resulted because Sunnis and Shiites could not agree upon a successor to Muhammed. Today, much of the conflict in the Middle East can be attributed to the Sunni and Shia sectarian divide. Politics is also affected by a lack of adequate governance and systemic corruption. This leads to political instability which serves as an incubator for terrorist and criminal organizations to spread and metastasize, much like a cancer. Adaptive factors are primarily driven by technology and counterterrorism tactics. As technology has evolved, jihadists have skillfully adapted to it and have adeptly used technology as a dangerous recruitment and fundraising tool. Likewise, terrorists have proven to be extremely adaptive to counterterrorism tactics, thereby sustaining their ability to continue their operations and to grow, as does a cancer.

### ABOUT BankersHub

**BankersHub** was founded in 2012 by [Michael Beird](#) and [Erin Handel](#), 2 Financial Services professionals dedicated to educating and informing banks, credit unions, solution providers and consultants in the U.S. and worldwide. BankersHub delivers best practices, research insights, opinions, economic trends and consumer views through online web education, virtual events and conferences, live streaming activities, custom training and content development.

For many years, al-Qaeda, the core organization, represented the most significant terrorist threat to the West. Following the 9/11 attacks, the United States (U.S.) and our allies took decisive steps to diminish al-Qaeda's operational capabilities. In 2015 and to date in 2016, the core al-Qaeda group has shown limited ability to function. However, al-Qaeda franchise groups, to include al-Qaeda in the Arabian Peninsula, which operates in Yemen, and the al-Nusra Front, which operates in Syria, have demonstrated that they are powerful regional terrorist threats but, not direct overt threats to the West. However, al-Qaeda in the Arabian Peninsula has twice unsuccessfully attempted to detonate bombs on U.S. bound aircraft.

The Jihadi movement in 2015, and now in 2016, has been dominated by the Islamic State in Iraq and the Levant (ISIL). In June 2014, ISIL took over considerable territory in Iraq and Syria and declared the formation of a caliphate. Since then, ISIL has amassed tremendous wealth and has recruited thousands of foreign fighters. ISIL was formerly known as al-Qaeda in Iraq and was one of the most formidable al-Qaeda franchises. ISIL and al-Qaeda have disavowed each other and are now bitter enemies and competitors. Currently, ISIL should be assessed on two levels. The first is for their operations and control within Syria and Iraq. The second is for their affiliated groups and operations outside of Syria and Iraq. By virtue of their relentless ability to use the internet to recruit foreign fighters and homegrown violent extremists, ISIL poses a noteworthy and concerning threat to Western society.

Because of their presence in Syria and the war against the Assad administration in Syria, both ISIL and the al-Nusra Front have been able to attract foreign fighters to join them. This recruitment has been greatly enhanced by ISIL and the al-Nusra Front's ability to use the internet to reach disenfranchised and otherwise susceptible individuals and those at-risk for recruitment. This is most notably true for ISIL. ISIL has been relentless with their recruitment propaganda and their kill, kill, kill messaging. The pool of troubled and impressionable individuals, regardless of whether they be either foreign fighters who leave their home countries to join ISIL, or who pledge allegiance to ISIL and stay home and operate as homegrown violent extremists, have emerged as the foremost concern to Western countries. These individuals are referred to as grassroots jihadists. They have emerged to pose a notable challenge for Western law enforcement and intelligence agencies. FBI Director, James Comey, has stated on numerous occasions that the FBI has ongoing investigations in all 50 States in the U.S. Likewise, FBI counterparts around the world are experiencing similar investigative challenges.

Director Comey has continuously emphasized how ISIL has trolled the internet, how they have identified potential recruits, and how they have bombarded these at risk individuals with constant email traffic to commit acts of terrorism. Once hooked, ISIL lures their potential recruits to encrypted chat rooms and attempts to complete the recruitment process. Law enforcement is not able to monitor the encrypted messaging. Director Comey has labeled this emerging phenomenon "going dark." Remember this term. "Going dark" is becoming one of the biggest terrorist challenges confronting law enforcement. The emergence of foreign fighters and homegrown violent extremists represents an alarming trend.

Take the case of Jalil Ibn Ameer Aziz, a 19 year old who was arrested on December 17, 2015. Aziz was charged with providing material support to ISIL. He lived with his parents and apparently spent most of his time on the internet. He wound up corresponding directly with ISIL recruiters in Syria. Aziz was unique in the sense he had no financial footprint. He did not work and lived with his parents. Among tasks he performed for ISIL, he assisted an individual who traveled to Turkey to join ISIL. Aziz facilitated correspondence between the aspiring foreign fighter and the ISIL recruiter in Syria. He did this from his parents' home in Harrisburg, Pennsylvania. Aziz reportedly used 57 Twitter accounts to espouse ISIL. He also allegedly posted the names and addresses of U.S. military personnel. He was arrested by the Joint Terrorism Task Force in Harrisburg at his parents' home. It was alleged he had four M-4 rifle magazine clips loaded with ammunition in his possession at the time of his arrest. No weapon was found. This begs the question: What was his intention for the ammunition? Was he planning to purchase or appropriate an

M-4 rifle? If so, what would his intent likely have been? Scary stuff! This is very concerning. More concerning is, how many more people are out there who fit this scenario?

## **Assessing the Ramifications of the Paris and San Bernardino Attacks**

The Paris and San Bernardino terrorist attacks were both attributed to ISIL in different ways. They both succeeded in attaining global media attention, resulted in gruesome deaths that shattered normally tranquil settings and caused considerable public fear and consternation. Despite their similar outcomes, the two attacks were vastly different. The Paris attacks were conducted by a combination of foreign fighters who returned home to France and Belgium and homegrown violent extremists recruited on the internet or through other individuals. ISIL directed and planned the attack from Syria. ISIL leaders were directly involved in the Paris attacks. There was a clear command and control structure. In contrast, the San Bernardino attack was carried out by a husband and wife who pledged allegiance to ISIL, but who carried out the attack on their own, influenced by, but not led by, ISIL. This is referred to as a leaderless attack.

It appears that the Paris attacks were funded in part by ISIL and in part by the attackers through their wages, entitlement funds or petty crimes. Media reports noted that prepaid cards were used by at least some members of the attack team. Syed Rizwan Farook was employed as a San Bernardino County health inspector. He had a steady income of over \$50,000. His salary undoubtedly paid for at least a portion of the attack. It was reported that Farook obtained a \$28,000 loan from an online loan company prior to the attack. There was speculation that loan proceeds may have contributed to paying for the attack.

With respect to both attacks, it is highly unlikely that transaction monitoring or other anti-money laundering (AML) alerting mechanisms would have identified unusual or suspicious activity by any of the attackers in Paris or San Bernardino. In looking specifically at the San Bernardino shooters, Farook and his wife Tashfeen Malik, they were a married couple with a daughter. Farook had a steady income for over five years; they rented a house and did not appear to display any AML red flags. The media speculated that because the loan obtained by Farook was done online, it lacked adequate due diligence. Again, regardless of the level of due diligence in this case, it is highly unlikely the loan company would have identified any red flags for suspicious activity.

Following both the Paris and San Bernardino attacks, political leaders vowed to destroy ISIL. Whether or not destroying ISIL is possible, the cancer of Islamic terrorism cannot be eliminated until the Sunni and Shia conflict can be truly understood and a treatment plan can be implemented to first reduce, and then ultimately, hopefully, eliminate the cancer. In addition, the lack of adequate governance in many Middle Eastern countries must be dealt with. The chaos and instability in these countries allows the cancer of Islamic terrorism to continue to grow. In part this is caused by the Sunni – Shia divide and in part by corruption, crime and other factors.

## **Proposed or Discussed Legislation**

As a result of the disclosure that prepaid cards were used to facilitate the Paris attacks, media reports stated that French legislators were considering introducing legislation to enhance compliance requirements for the purchase of prepaid cards. In the aftermath of San Bernardino, U.S. Congressional representatives have questioned the loan due diligence process and have mentioned the potential for new legislation. In addition, in response to the San Bernardino attack, Congresswoman Maxine Waters reintroduced legislation she sponsored last year to hold bank executives accountable for anti-money laundering standards. Also, the House Financial Services Committee's Terrorist Financing Task Force is expected to introduce terrorist financing legislation.

Before introducing any new legislation, legislators in France, the U.S. and other countries should think before they act. They should ask themselves if additional AML legislation is actually warranted. They should take the time to reasonably assess existing legislation and discuss potential legislative needs with law enforcement, regulators and most importantly with financial institution compliance officers and other industry representatives and experts. In the case of France, would legislation regarding prepaid cards have precluded the Paris attackers from using prepaid cards? The answer most likely would be no. In the case of San Bernardino, would enhanced due diligence requirements regarding online or other loans have precluded Farook from receiving a loan or resulted in the identification of suspicious activity? The answer would most likely be no. Would terrorist financing legislation have prevented the San Bernardino attack from happening? Again, the answer would most likely be no.

## **How Should Financial Institutions Respond to Terrorist Incidents?**

As noted above, it is highly unlikely that homegrown violent extremists and, to a lesser degree, foreign fighters can be identified through transaction monitoring or normal AML filters. Banking activity involving grassroots jihadists will most likely involve legitimate employment compensation or petty crimes that can be reasonably explained for due diligence purposes. In most instances, financial institutions would not identify having facilitated a terrorist as a customer until after the fact. Negative news hits are not likely until an attack takes place, is attempted, or when law enforcement disrupts a plot and the attacker or would be attacker is identified.

When events like Paris and San Bernardino take place, financial institutions typically run the names identified through their systems. In the event name matches, as customers or for transactional activity occur, financial institutions usually take the appropriate actions and notify law enforcement immediately. This is a reactive mechanism valuable to law enforcement. Representatives from the FBI's Terrorist Financing Operations Section (TFOS) have stated at various AML conferences that financial institutions have been extremely responsive to all terrorist incidents in a productive reactive fashion. This process can and should be enhanced. Financial institutions should consider adopting the law enforcement SWAT Team concept.

A Special Weapons and Tactical (SWAT) Team is a group of highly trained police officers who deal with extremely dangerous criminals. The Los Angeles Police Department first formed a SWAT Team in 1967. Today, most law enforcement agencies in the U.S. and internationally have SWAT Teams. SWAT Teams are regularly deployed to deal with extremely dangerous and violent criminal confrontational situations. SWAT Team members receive regular and intensive specialized training to deal with the challenging situations they are confronted with. SWAT duties are normally collateral to the primary investigative responsibilities of the law enforcement officer.

Analogous to the SWAT Team concept, financial institutions should form Strategic and Tactical Response (STR) Teams to deal with a Bank Secrecy Act (BSA)/AML response to situations they designate as emergency response situations, such as terrorist attacks. The STR Team should be comprised of specially trained BSA/AML investigators and/or analysts as conducive to the size and capacity of the financial institution. STR Team responsibilities should include:

- Regular and specialized training regarding terrorism, terrorist financing and other situations designated as emergency response situations by the financial institution
- Conducting “urgent” reactive investigations following a violent event designated as an emergency response situation by the financial institution
- Establishing and maintaining a close working relationship with appropriate law enforcement agencies responsible for investigating terrorist and other emergency response situations
- Conducting after action reviews to assess the timeliness and effectiveness of investigations and event law enforcement liaison
- To the extent practical, conduct proactive and targeted monitoring initiatives to identify homegrown violent extremists, foreign fighters and terrorist related transactional activity

The formal financial system serves as both a facilitation tool and a detection mechanism for terrorists and criminals. Effective STR Teams will greatly enhance the possibility of detection. Experienced STR Teams with established law enforcement contacts would be in a position to provide more timely and valuable financial information during emergency situations. In the event that an investigation into situations like Paris and San Bernardino are ongoing and all subjects have not been identified, the timelier the flow of meaningful financial information, the more likely all subjects will be identified as expeditiously as possible.

## Conclusion

As terrorism trends continue to evolve through inherent and adaptive factors, detective mechanisms become more important. Finance is one of the most significant vulnerabilities confronting terrorists. Following a terrorist incident, or in attempting to establish proactive and preventative strategies, knowing what financial information is relevant, where to collect it from, and how to use it are facts all law enforcement investigations will benefit from. Despite the many challenges that exist, STR Teams can point law enforcement to the relevant financial information required to respond, counter, deter and prevent terrorists from succeeding.

The first SWAT Team was formed in 1967. Today SWAT Teams are an integral component of effective law enforcement responsiveness to dangerous criminal situations. The STR Team concept has the same potential. Financial institutions play an important role in providing law enforcement with valuable financial intelligence. In establishing STR Teams, financial institutions will become a more integral component for denying terrorists and violent criminals from exploiting the financial system in furtherance of their illicit activities.

# Coming Soon to a Computer Near You!

Click on the Topic to Learn More and Register



**3-Part Webinar Bootcamp**  
**Same Day ACH**  
**Preparing for the**  
**Changes Ahead**  
**April 5/12/19, 2016**  
**2:00 – 3:00 PM ET**

**3 Webinars with Playbacks!**

- Beginning Implementation of Same Day
- Exceptions and Operational Challenges
- Risk Mitigation Best Practices



**David Peterson**  
*Founder – i7 Strategies*

April 26 – 28, 2016  
12:00 pm – 1:00 pm ET

**Transforming Branches from**  
**Transaction to Engagement**  
*Strategic Customer Planning for*  
*Banks and Credit Unions*

**3-Part Live Online Bootcamp**



**3-Part Webinar Bootcamp**  
**ACH Bootcamp**  
**What Financial Services**  
**Professionals must know**  
**April 26 - 28, 2016**  
**2:00 – 3:00 PM ET**

**3 Webinars with Playbacks!**

- ACH Basics and Exception Item Handling
- Risk Management for ODFI and RDFI
- Audit, Risk Assessment and Regulations



**Ripped From Today's Headlines**  
**Terror Financing and Money Laundering**  
**What Financial Institutions MUST Understand and Do NOW**

**JUNE 6, 2016**  
**12:00 - 1:00 PM ET**



**Brussels**  
**TERROR ATTACKS**

**Dennis Lormel**  
*Founder and President*  
*DML Associates*  
*Former Advisor*  
*Congressional Anti-Terrorist*  
*Financing Task Force*

[More Info](#)