On December 10, the Chapter held its fourth annual “Year-in-Review” followed by a holiday networking reception. The event featured two panels (one comprising industry practitioners and the other law enforcement) followed by a speaker from Capitol Hill on the legislative perspective.

The first panel of industry practitioners was composed of Sepideh Behram (Burke & Herbert Bank), Les Joseph (Wells Fargo) and Rachel Carpenter (MGM National Harbor) and moderated by John Byrne (AML RightSource). Speakers discussed their areas of focus in 2018 and priorities for 2019. For the first time, the private sector panel also included a speaker from the casino industry. She provided detailed insight into the comprehensive AML regime in place to meet regulatory objectives. She articulated that the biggest challenge in 2019 is getting clarification on marijuana-related businesses (MRBs) and on-line sports wagering. She also indicated that regulatory relief should focus on structuring SARs, which continues to be the top category of filing. The bankers on the panel agreed that MRBs present challenges in banking and anticipate this to be a priority in the coming year. In addition, the bankers projected that continued emphasis on innovation and artificial intelligence are on the horizon along with an increased examination focus on customer due diligence and beneficial ownership.

The second panel was composed of Todd Porter (Assistant Section Chief, Counterterrorism Division, Terrorist Financing Operations Section, FBI), Leo Tsao (Chief of the Bank Integrity Unit, Money Laundering and Asset Recovery Section of the Criminal Division, United States Department of Justice), Kathy Enstrom (Director of Operations, Policy, and Support for the Internal Revenue Service’s Criminal Investigations unit) and moderated by Dennis Lormel (DML Associates) and they focused on law enforcement and their perspective on 2018 and projections for 2019. The FBI representative commented that home-grown violent extremists are the greatest threat today. The nature of this threat moves faster today than ever before. DOJ is focusing on transnational criminal organizations, the opioid epidemic and terrorism. IRS – Criminal Investigation’s (IRS-CI) priority for 2019 is data analytics—using data to identify cases more quickly. FBI priorities include microfinancing and cryptocurrency.

Jared Roscoe, senior banking counsel for Senator Mark Warner, provided his perspective on the problems Congress is trying to address in drafting AML reform legislation and he outlined potential “common sense” reforms under consideration. Congress has taken up this issue, in part,
because CEOs rank AML burden as one of their top priorities. Problems include a lack of coordination amongst law enforcement, financial institutions, and regulatory agencies both state and federal; a failure to let financial institutions embrace new technology; and de-risking.

Reforms that he believes can get bipartisan support include:
- institutionalizing regular feedback mechanisms;
- improving examination priorities;
- giving law enforcement a seat at the table when setting priorities;
- encouraging technological innovation;
- requiring corporate entities to report beneficial ownership information; and
- permitting financial institutions to share information with their foreign affiliates, leading to better SARs and fewer false positives.

Any AML reform efforts will need to be cognizant of privacy concerns. He believes the time is ripe on the Hill for updating the AML framework. The pace of hearings has increased and there is a lot of broad bipartisan consensus that reform is needed. The Administration is engaged on the topic, but it will take a push from all sides to get something done.

**IRS-CI TELECOMMUNICATIONS INVESTIGATIONS**

Christopher Westphal

On November 7, 2018, event participants had the opportunity to hear from Christopher Westphal from IRS-Criminal Investigations (IRS-CI) details of a case investigation worked jointly with IRS-CI, Department of Homeland Security Investigations (HSI), Department of Justice’s Money Laundering and Asset Recovery Section and Foreign Corrupt Practices Unit and the US Attorney’s Office for the Southern District of New York (SDNY).

Vimpelcom (VIP), a multinational telecommunications company headquartered in Amsterdam, Netherlands, was alleged to have engaged in an international conspiracy which included a series of complicated monetary transactions to launder corrupt proceeds. Specifically, VIP was charged with paying bribes to the daughter of then President of Uzbekistan for the purpose of gaining initial entrance into the Uzbekistan telecommunications market. According to the charges, subsequent bribe payments were paid for the purposes of continuing operations, gaining lucrative telecommunications frequencies and sustaining an amicable relationship with the Uzbekistan government/telecommunications regulator. The alleged bribery payments were laundered through the use of shell companies, nominees, and use of financial accounts in countries with poor oversight and AML practices.

In February 2016, VIP entered into a Deferred Prosecution Agreement (DPA), with SDNY while VIP’s Uzbekistan subsidiary – Unitel – pled guilty to conspiracy to violate the FCPA and falsifying books and records. Pursuant to the DPA, VIP paid a criminal penalty of $460 million. The SEC also assessed VIP fines, penalties and disgorgement of approximately $350 million. Lastly, pursuant to the DPA, VIP was required to agree to a monitorship.

The investigation is ongoing and focusing on potential violations committed by employees of VIP.

**Second Annual Community Bank and Law Enforcement Fusion Forum**

Mary Bashore

The Second Annual Community Bank and Law Enforcement Fusion Forum took place on August 29th and provided an opportunity to share perspectives amongst law enforcement, the intelligence community, banking regulators and industry representatives.
A slate of top-notch speakers addressed current trends, emerging threats, concerns and considerations, regulatory hot topics and human trafficking. Recurring themes among nearly all the speakers were cyber threats and the need for public/private partnerships.

Regarding current trends, the key challenges faced by all participants are to keep up with technology, and to change existing tools and approaches, understanding that newer payment systems enable criminals to engage in nefarious activities with great speed. Expanding public/private partnerships is essential to meet the challenges from a national security perspective as well as to address strategic risk from the bank perspective. We know the cost of compliance is huge, but too many institutions are paying the cost of getting it wrong.

Dan Stipano, former OCC deputy chief counsel, believes that FinCEN should revisit its guidance on information sharing, and that the ability to share information “consistent with the purposes of the BSA” should be made broader.

Tim Murphy, formerly Deputy Director of the FBI, spoke of “the failure of imagination” in that our efforts are largely based on a 30-year-old construct that does not meet the fundamental needs of the current environment. Alternate payment systems, estimated at $4 trillion per year, may soon overtake the traditional U.S. financial system as the dominant global financial system.

Looking forward, John Byrne, Vice Chairman at AML RightSource, stated that any organization with a financial footprint should have AML responsibility, including the real estate industry, attorneys and other “gatekeepers.” To date there has been strong pushback from these industries. He also mentioned proposals to increase the thresholds for SAR and CTR filing in draft legislation on the Hill. It is not clear what benefit would be derived from these changes as financial institutions generally have efficient systems in place, and it would certainly be costly for them to make significant changes. In addition, law enforcement has strong objections to raising these thresholds. Speakers suggested that innovation and revisiting the CTR exemption processes could have a positive impact.

Tim Murphy and John Byrne shared their views on “de-risking” and the consequences of driving potentially higher risk accounts to smaller institutions, which may not have the capability to manage the risk effectively. Collateral damage occurs when charities and humanitarian organizations are unable to sustain worthwhile activities, especially in developing countries. This causes some groups to go underground, entirely bypassing formal financial systems. ACAMS is working with the World Bank as well as NGOs to alleviate this problem.

On the law enforcement panel, Kelly Jackson, IRS-CI, emphatically stated “if it’s suspicious, file” regardless of the minimum dollar threshold. Her point was that a small transaction or pattern of activity could be the “tip of the iceberg” tied to a major case involving many other institutions. Plus, if there is a suspicion of tax evasion the IRS will want to couple the bank information with tax data as investigations of transnational organized crime often revolve around tax evasion cases.

Our law enforcement partners continually emphasize SAR best practices, the all-important narrative, and the fact every single SAR is reviewed by a team composed of a cross-section of law enforcement personnel. They often focus on key words. It was suggested financial institutions list the supporting documents pertaining to the case in the SAR so law enforcement knows what to ask for as they pursue their cases. Banks should file an amended SAR if new information becomes available, referencing the prior SAR.
The lunch speaker, Mike Loughnane of Loughnane Associates, advised thinking in terms of value rather than just money. Financial crime may entail kidnapping or malware for ransom and with the proceeds being laundered using sources outside the financial industry, such as via purchase of cars, real estate, jewelry, or artifacts. Although traditional tools continue to be used by money launderers to obtain, transfer and use illegal funds, criminals may adjust to increased pressure by changing jurisdictions or methods.

The new beneficial ownership rule is the top regulatory examination hot topic. Financial institutions should have policies and procedures in place, but must ensure they are consistently applied. Most institutions understand what is needed for account opening, but “triggering events” must not be overlooked.

Banking regulators are increasing their emphasis on model validation, as well as tuning and calibration of settings and parameters. Per Jill Apa of the FDIC, automated processes require data integrity, comprehensive capture of data, reasonable parameters, and extensive customer history in order to detect anomalies. Most importantly, human judgment is needed to assess all the available information; this often requires more, not less, staff to operate an automated system properly.

The FinCEN representative, Gary Novis, gave some statistics showing that cybercrime filings are way up. He noted the need for an institution’s fraud, security, AML/BSA and IT departments to work together and respond quickly.

Later, Dennis Lormel of DML Associates spoke about human trafficking and exploitation of labor. He told of his experience as an FBI special agent with a criminal engaged in prostitution, how frustrating it can be to combat these crimes, and how often we can see it around us if we have situational awareness. Polaris (an NGO focused on stopping human trafficking) and ACAMS have formed a working group fighting to end modern slavery. They have identified 25 typologies which banks can build into their monitoring platforms. We are reminded to update the ever-growing list of red flags we build into our systems to be an effective detection mechanism rather than a facilitator of criminal activity.

**Money Laundering via Cryptocurrencies**
Bob Pasley

On July 18, a panel of government and private sector experts on cryptocurrencies, composed of Ross Delston, Lourdes Miranda and John Rollins, discussed the regulatory and enforcement perspectives related to cryptocurrencies, including the technical aspects of cryptocurrencies, and the intelligence and investigatory procedures applicable to cryptocurrencies. They explained that, although there are some legitimate reasons to want to be anonymous, cryptocurrencies are attractive to criminals because, among other things, they promote some – but not complete – anonymity and are subject to limited government involvement. The cryptocurrency world sees fiat currency (legal tender backed by a central government) as a competitor.
We learned that most banks, in fact, view cryptocurrencies as high risk, but that the Financial Action Task Force (FATF) has not issued any applicable international standards vis-à-vis this risky area of financial transactions. However, the panel noted that the Financial Crimes Enforcement Network (FinCEN) treats cryptocurrency exchangers and administrators as money services businesses (MSBs) and requires them to register as such and to maintain an AML program that contains what we all know as the “four pillars.” However, in the speakers’ view, these entities will not do a good job of AML compliance, in part, because it is a relatively new system and there are not a lot of red flags at this point for suspicious activity. Cryptocurrency exchangers and administrators are also subject to IRS BSA examinations. To date, FinCEN has imposed civil money penalties on two cryptocurrency exchangers for BSA violations.

The panel explained that cryptocurrencies can be used for money laundering and, specifically, that the various stages pertaining to cryptocurrencies – known as mixing, shifting and exchanging – are reflective of the three well-known stages of money laundering. How much of the cryptocurrency market is composed of fraudsters and manipulators remains to be seen, but it is clear that the opportunities for misuse, fraud, and financial crimes are plentiful.

Some of the conclusions set forth by the panel are that cryptocurrencies can pose a risk of money laundering and terrorist financing; that criminal activity involving cryptocurrencies is difficult to detect; that FinCEN, and law enforcement in general, are paying close attention to the risks posed by cryptocurrencies and that exchangers and administrators therefore should be prepared for greater scrutiny.

Panel Discussion on Terrorist Financing and Financial Crime Prevention
Megan Jeffries

On October 25, the U.S. Capital Chapter hosted a panel discussion sponsored by Thomson Reuters and Refinitiv and featuring moderator Dennis Lormel, President & CEO, DML Associates. The panelists were Marcy Foreman – Managing Director, Global Investigations Unit, AML Compliance, Citi; Todd Porter, Assistant Section Chief, Terrorist Financing Operations Section (TFOS), FBI; and Jesse Spiro, Global Head of Threat Finance & Emerging Risks, Refinitiv. The discussion blended expertise in technology, law enforcement, and private bank investigations—representing the critical elements of addressing existing and evolving threats.

The primary goal of Counter-Terrorism is to stop a terrorist attack before it happens and, secondly, to respond quickly when an attack does happen. The threat of terrorism today is dynamic and complex. Threats include traditional terrorism threats—large spectacular events, such as those perpetrated by Al Qaeda or ISIS. These attacks are prevented by in-depth understanding of the patterns of communication, travel, propaganda, and financing—information driven by financial intelligence and a deep understanding of the terrorist operating network. However, the greatest threat today is the homegrown violent extremist; these perpetrators are commonly known as lone-wolves. These extremists are typically self-radicalized U.S. citizens and plan their attacks within days or hours of the execution, a short “flash-to-boom.” There is little, if any, time to connect the dots between red flags and the terrorist event. Real-time collaboration with the private sector is crucial for counter-terrorism given a key aspect of these investigations being reliant on big data analysis, specifically financial transactions.

Financial intelligence including personally identifiable information (PII), contact information, and patterns of activity are always extremely valuable to law enforcement and can be used to develop typologies to flag potential terrorist risks. In the current counter-financing of terrorism (CFT) environment, behavioral analysis plays a crucial role due to the low dollar value and volume of the transactions. A case discussed involved a woman arrested in Ohio for materially supporting al-Qaeda and providing training to home-grown extremists. She believed that sending money is the same as
doing “jihad.” She provided advice to extremists on remittance instructions, advising them to use a fake name and not send all the money at once, but rather low denominations such as $200 or $300 at a time.

The panel reiterated the importance of banks leveraging information sharing between financial institutions and law enforcement to build this partnership. Challenges to information sharing exist particularly when encountering privacy laws which can detrimentally impact this partnership and the availability of critical information. As technology advances and third-party vendors have the ability to scrape data and provide a broad array of information such as associates or beneficial ownership, the investigative time frame is reduced. These types of resources enable a financial institution to have improved insight and knowledge about their customers and become aware of instances where a customer may be using multiple institutions to further their criminal intent.

The panel agreed that establishment of an effective private and public partnership is critical to an effective BSA/AML program to bring together the financial data from private sector, machine learning and big data capabilities of third-party solutions and law enforcement’s investigative skills.

Thank you to our speakers and sponsors: Jill Apa, Sepideh Behram, John Byrne, Rachel Carpenter, Mike Caswell, Ross Delston, Scott Dueweke, Kathy Enstrom, Marcy Foreman, John Gervino, HHS NOC Training Center, Kelly Jackson, Les Joseph, KPMG, Dennis Lormel, Mike Loughnane, Lourdes Miranda, Tim Murphy, Tami Newit, Gary Novis, Orrick Herrington & Sutcliffe, Todd Porter, Refinitiv, John Rollins, Jared Roscoe, Safe Banking Systems LLC, David Schiffer, Jesse Spiro, Dan Stipano, Thomson Reuters, Leo Tsao, and Christopher Westpahl.