

**Testimony of  
Dennis M. Lormel  
President & CEO  
DML Associates, LLC**

**Before the  
United States Senate  
Committee on Banking, Housing, and Urban Affairs**

**At the Hearing *“Combating Money Laundering and Other Forms of Illicit Finance: Opportunities to Reform and Strengthen BSA Enforcement”***

**January 9, 2018**

Good morning Chairman Crapo, Ranking Member Brown and distinguished members of the Committee. Thank you for the opportunity to testify before you today. My name is Dennis M. Lormel. I have been engaged in the fight against money laundering, financial crimes, terrorist financing and other forms of illicit finance for 45 years. I served in the U.S. Government for 31 years, 28 of which I served as a Special Agent in the Federal Bureau of Investigation (FBI). I amassed extensive investigative experience in complex and labor intensive financial investigations as a street agent, first line supervisor, middle manager and senior executive. In 2000, I was promoted to Chief of the Financial Crimes Section, in the FBI’s Criminal Division. Following the terrorist attacks of September 11, 2001, I formulated, established and led the Terrorist Financing Operations Section (TFOS) within the FBI’s Counterterrorism Division. During my FBI career, I was the direct beneficiary of Bank Secrecy Act (BSA) data to include currency transaction reports (CTRs) and suspicious activity reports (SARs). I experienced firsthand the value BSA data brought to investigations. This was especially true after 9/11. One of our important initiatives was a datamining project which included SAR reporting. For the past 14 years, I have been a consultant, primarily working in the financial services industry, in the anti-money laundering (AML), terrorist financing and financial crimes prevention community. In this capacity, I have worked with private sector clients to improve the effectiveness and efficiency of BSA reporting.

My government investigative and private sector consulting experience has provided me a unique opportunity to understand and appreciate two very distinct perspectives regarding the BSA. Two of the principal stakeholders of the BSA are law enforcement and financial institutions. Putting this in the context of the flow and utilization of financial information, law enforcement is the backend user and beneficiary of BSA data. Financial institutions serve as the frontend repository and custodian of financial intelligence. Financial institutions also serve the critical function of being the monitor for identifying and reporting suspicious activity and other BSA data to law enforcement. Simply put, law enforcement uses BSA data to predicate or enhance investigations from a tactical standpoint. Law enforcement also uses BSA data for strategic purposes. From a simplistic standpoint, the flow of BSA data that is continuously filtered to law enforcement is invaluable. When you layer the complexities of regulatory compliance requirements over the monitoring and filtering process financial institutions must follow, the

effectiveness and efficiency of BSA reporting from the frontend monitor to the backend beneficiary, becomes flawed.

My point is that the BSA system is not broken. The system is fraught with many inefficiencies but it works. Law enforcement consistently receives valuable intelligence from BSA data. The challenge is that the BSA system can and should be much more effective and efficient. In this context, I applaud the Committee for dedicating the time to assess the effectiveness and efficiency of BSA enforcement and considering reform measures to strengthen BSA reporting requirements.

I'd like to take the opportunity to commend the Clearing House for having issued their report in February 2017 "A New Paradigm: Redesigning the U.S. AML/CTF Framework to Protect National Security and Aid Law Enforcement". I believe the report is a good point of reference to initiate discussion for reform consideration. I laud the Clearing House for recognizing the importance of including all stakeholders in the discussion. I was not involved in the two symposiums held to formulate the report. One concern I have about the report is the actual extent to which law enforcement was included as a contributing stakeholder. In my view, law enforcement is the most important stakeholder because the BSA was intended to assist law enforcement. When the report was issued, I contacted then current law enforcement executives in positions like I held and none were included in the deliberations. I encourage the Committee to include a variety of active and former law enforcement executives in your ongoing dialogue and efforts to strengthen the BSA.

The BSA was passed in 1970 with the legislative purpose of generating reports and records that would assist law enforcement in following the money and developing prosecutable criminal cases. Since passage of the BSA, additional legislation has periodically been enacted to enhance regulations. Most notably, passage of the USA PATRIOT Act established a host of new measures to prevent, detect, and prosecute those involved in money laundering and terrorist financing. Going forward, deliberations to enhance the BSA should focus on systemic vulnerabilities, evolving technology, emerging trends and opportunities to leverage public and private partnerships and information sharing with an eye on continuing to enhance law enforcements investigative ability.

As noted in the introduction of the BSA, "the implementing regulations under the BSA were originally intended to aid investigations into an array of criminal activities, from income tax evasion to money laundering. In recent years, the reports and records prescribed by the BSA have also been utilized as tools for investigating individuals suspected of engaging in illegal drug and terrorist financing activities. Law enforcement agencies have found CTRs to be extremely valuable in tracking the huge amounts of cash generated by individuals and entities for illicit purposes. SARs, used by financial institutions to report identified or suspected illicit or unusual activities are likewise extremely valuable to law enforcement agencies". This statement is a true reflection of BSA reporting. However, there is a troubling backstory about perceived regulatory expectations that have resulted in systemic inefficiencies.

Regardless of the extent or effectiveness of BSA regulations, criminals and terrorists must use the financial system to raise, move, store and spend money in order to sustain their illicit operations and enterprises. The reality is that no matter how robust an anti-money laundering (AML) program is, it cannot detect all suspicious activity. The BSA standard is that financial institutions maintain AML programs that are reasonably designed to detect and report suspicious activity. One of the regulatory challenges confronting financial institutions today is the question: What constitutes a reasonably designed AML program? Regulatory expectations, either real or perceived, have caused financial institutions to lose sight of the purpose of BSA reporting and have consequently led to many of the systemic inefficiencies of BSA reporting.

In using the financial system, criminals and terrorists are confronted with distinct contrasts. On one hand, the financial system serves as a facilitation tool enabling bad actors to have continuous access to funding. On the other hand, the financial system serves as a detection mechanism. Illicit funds can be identified and interdicted through monitoring and investigation. Financing is the lifeblood of criminal and terrorist organizations. At the same time, financing is one of their major vulnerabilities. At the basic core level of the frontend and backend data process flow, BSA reporting works and is more apt to serve as the intended detection mechanism. The more convoluted and distracting the regulatory process becomes, the greater the likelihood that the financial system serves as a facilitation tool for criminals and terrorists.

There are a number of vulnerabilities or high risk areas in the financial system that criminals and terrorists exploit. I categorize them as criminal activity and facilitation tools bad actors use to exploit their ill-gotten gains derived from their criminal activity. The biggest crime problems we encounter include fraud and money laundering. Most criminal activity, other than select violent crimes, includes elements of fraud and money laundering. Drug trafficking, human trafficking, corruption and other crimes contain elements of fraud and require money laundering. Some of the more significant facilitation tools include wire transfers, correspondent banking, shell companies (beneficial ownership), illegal money remitters (informal value transfer systems), non-government organizations, credit and debit cards, and electronic mechanisms. In my experience, one of the biggest areas of vulnerability in the financial system is identifying illegal money remitters.

One facilitation tool that consistently garners Congressional attention is the issue of beneficial ownership. Year after year, potential bills are introduced regarding beneficial ownership. I strongly encourage the Committee to consider beneficial ownership legislation as an enhancement to the BSA. Throughout my law enforcement career, I dealt with the challenge of shell companies and identifying true beneficial owners. Based on my experience, I believe beneficial ownership should be required by Secretaries of States, at the point of incorporation. On May 11, 2016, the Financial Crimes Enforcement Network (FinCEN) issued Customer Due Diligence Requirements for Financial Institutions (the CDD Rule). The rule strengthens existing customer due diligence (CDD) requirements and requires banks to identify and verify the beneficial owners of legal entity customers. Financial institutions are in the process of implementing CDD requirements. If identification of beneficial ownership were required at point of incorporation, the burden on financial institutions would be lessened.

Regarding the BSA, it is important that all stakeholders be engaged in the discussion and deliberation to improve the effectiveness and efficiency of BSA reporting and enforcement. More importantly, all stakeholders should be involved in breaking down real or perceived regulatory impediments. In each of our areas of responsibility, all BSA stakeholders should strive to exploit the financial vulnerability of criminals and terrorists by ensuring the financial system serves as a detection mechanism disrupting illicit funding flows. Although the BSA system works, it is flawed and lacks the effectiveness and efficiency it was intended to achieve.

The starting point toward improving the effectiveness and efficiency of BSA reporting is to improve the current system through building meaningful and sustainable public and private sector partnerships beginning with BSA stakeholders, including the financial services industry, regulators, policy makers, sanctioning authorities, intelligence experts, law enforcement, legislatures and other stakeholders. We need to start by improving the efficiencies of our current system by breaking down impediments. We then need to determine what enhancements to regulations should be considered.

Building meaningful and sustainable partnerships begins with understanding perspectives. Each stakeholder partner possesses a perspective based on their professional responsibilities and experience. Each of our perspectives will be somewhat unique. Understanding and blending the perspectives of our partners will enable us to establish a middle ground to improve or build efficiencies upon. As this process evolves, we can leverage the capabilities and capacity of our partners. This type of evolution sets the stage for developing innovative ideas and proactive measures.

One of the inherent disadvantages we have in our financial system and AML environment is that we are reactive. Criminals and terrorists have the advantage of being proactive. Our ability to add innovative ideas and proactive measures to an otherwise reactive system can achieve impactful investigative results. In fact, there have been recurring innovative and proactive law enforcement investigations. I speak from firsthand experience when I talk about developing proactive techniques. I can point to specific proactive law enforcement initiatives following 9/11 that were the direct result of innovative public and private sector partnerships. My emphasis here is we can be innovative within the current framework. We can also improve the current landscape through enhancements to encourage and/or incentivize innovation. For example, financial institutions conduct baseline transaction monitoring to alert to anomalies that can lead to identification of suspicious activity. By developing rule sets and scenarios that are targeted to specific transactions or financial activity, we are more likely to identify specific or targeted suspicious activity regarding specific crime problems such as human trafficking. Financial institutions are reluctant to employ targeted monitoring initiatives because of concern for the potential regulatory expectations or other perceived impediments such innovative thinking could incur.

Included as an attachment to my testimony is an article I wrote in 2011 for publication by the Association of Certified Anti-Money Laundering Specialists (ACAMS) titled "Perspectives, Partnerships and Innovation". As an example of innovative and proactive targeted monitoring, the article details the public and private partnership of a special AML investigative team at JPMorgan Chase (JPMC) in 2009, with Homeland Security Investigations (HSI), Immigration and Customs Enforcement (ICE). I provide

extensive training to the financial services industry regarding AML, terrorist financing, fraud, investigations, suspicious activity reporting and related topics. I frequently cite the JPMC and ICE collaboration as one of the best models for partnerships and innovation. One of the accomplishments of this collaboration was the effective and efficient use of BSA data based on targeted monitoring against human trafficking. The attached article also provides a sense of leveraging perspective and, the regulatory and collateral challenges financial institutions face by endeavoring to be innovative.

As an extension of public and private partnerships, we should consider how to improve information sharing. The PATRIOT Act provided us with information sharing vehicles such as Section 314(a) where financial institutions can share financial information with law enforcement and Section 314(b) where financial institutions can share information with each other. Efforts should be made to enhance Section 314 information sharing in the current environment. In addition, any proposed enhancements to the BSA should consider additional information sharing mechanisms. The more we can do to enhance information sharing, the more meaningful information will be for law enforcement and the more detrimental to criminals and terrorists. During their plenary session in June 2017, the Financial Action Task Force (FATF) stressed the importance of information sharing to effectively address terrorist financing. I have always been a huge proponent of information sharing to the extent legally allowable.

One of the most productive examples of public and private sector partnership, and information sharing, is the Joint Money Laundering Intelligence Task Force (JMLIT) in the United Kingdom (UK). JMLIT was formed by the government National Crimes Agency (NCA) in partnership with the financial sector to combat high end money laundering. JMLIT was established as a business-as-usual function in May 2016. It has been developed with partners in government, the British Bankers Association, law enforcement and more than 40 major UK and international banks. I'm hopeful that the U.S. can assess and work through information sharing and privacy concerns in order to replicate the UK JMLIT model.

With respect to terrorist financing, any legislative enhancement to the BSA should consider facilitating obtaining security clearances for select financial institution personnel. In most instances, law enforcement is precluded from sharing classified information with financial institutions. If financial institutions had select personnel with a security clearance and they could gain access to select classified information, they would be able to either search for specific financial information or establish targeted monitoring initiatives to identify specific financial intelligence that would be meaningful to classified or otherwise sensitive counterterrorism investigations.

Throughout my career, I have worked closely with financial institution AML and fraud compliance professionals. I have the utmost respect for their dedication and commitment to protecting the integrity of their financial institutions and for identifying the misuse of the financial system by bad actors. Next to my former law enforcement colleagues, I hold my friends in AML and fraud compliance in the highest regard. It is important to note that the BSA shortcomings we face are systemic problems caused by multiple factors and not by groups of individuals.

One of the positive trends evolving within financial institutions, in part, founded on the dedication factor of AML professionals that I complimented, is the formation of financial intelligence units and/or special

investigations teams established to deal with terrorist financing and emergency response situations such as the Panama Papers, the FIFA scandal and human trafficking. In addition to developing proactive mechanisms, like targeted monitoring, these teams have developed “urgently” reactive capabilities to respond to terrorist and emergency situations requiring immediate response. As I mentioned earlier, AML programs are inherently reactive. One of the best reactive mechanisms we possess is negative news reporting. For example, when terrorist incidents like the attacks in New York in October and December 2017 occurred, as soon as the names of the perpetrators are announced, these special investigations teams immediately run the perpetrator names through their systems and should they identify accounts or transactional activity involving those individuals, they immediately contact law enforcement.

Like the JPMC and ICE human trafficking targeted monitoring program I mentioned, I’m aware of a major bank that has formed a special investigative team to similarly search for human trafficking that could be related to a forthcoming major sporting event. I’m not at liberty to further identify the financial institution or circumstances. However, it is important to note that financial institutions and law enforcement do participate in targeted monitoring projects and when they are able to do so, BSA data flows from the frontend monitor (a financial institution) to the backend beneficiary (law enforcement) in a timely and, effective and efficient manner.

I encourage all financial institutions to establish special investigations or critical incident response teams. I teach and view these teams analogous to law enforcement Special Weapons and Tactics (SWAT) teams. SWAT officers receive regular intensive training to deal with dangerous emergency response situations. Most SWAT officers have other primary law enforcement assignments, and SWAT is a collateral duty. Financial institution SWAT or critical incident response or special investigations teams should also receive special training for dealing with emergency response and targeted proactive investigative situations. Regardless of the size of a financial institution, all financial institutions should establish special investigative teams to identify and report targeted suspicious activity. Whether the team is a unit or one investigator, all financial institutions should develop emergency response capabilities.

In my training programs regarding money laundering, fraud and terrorist financing, I stress the importance of situational awareness. Situational awareness is being aware of and responsible for your physical surroundings regarding your personal safety and security. If you see something, say something. The same principles apply to money laundering, fraud and terrorist financing. You need to be situationally aware of and understand the flow of funds for illicit purposes. Much the same, we all need to be situationally aware of the vulnerabilities to the financial system and ensure the BSA is as effective and efficient as it can be.

The most important BSA report is a SAR. In most instances, the biggest regulatory compliance breakdown resulting in some sort of enforcement or regulatory action is the failure to file SARs or to adequately file SARs. I cannot underscore enough that law enforcement is the direct beneficiary of SARs. Regardless of systemic inefficiencies, law enforcement consistently benefits from SAR filings.

SARs are used tactically to predicate and/or enhance criminal investigations. SARs are also used strategically for analytical purposes. When attempting to measure effectiveness and efficiency of SAR filing, we cannot solely rely on the percentage of SARs filed versus the number of SARs used to predicate or enhance an investigation. We must also factor in how SARs are used strategically for trend analysis and analytical purposes. Finding accurate metrics to determine the effectiveness and efficiency of SAR filing is extremely difficult.

When I was in law enforcement, I used SARs for both strategic and tactical purposes. When I was Chief of TFOS at the FBI, we established a financial intelligence unit. I wanted to know on a recurring basis what were the emerging threat trends, as well as emerging crime problems. SARs were one of the data sets we used for such trend analysis. We also used SARs for tactical purposes in furtherance of investigations. We used financial intelligence, some of which was derived from BSA data, to include SARs and CTRs, for tactical proactive investigations and for tactical reactive or more traditional “books and records” “follow the money” investigations. We used datamining technology for both strategic and tactical initiatives. I believe that the FBI continues to use BSA data for strategic and tactical investigative purposes.

I developed a flow chart I use for training purposes describing the “lifecycle” of a SAR. It tracks a SAR from the point of origin when it’s filed with FinCEN through both regulatory and law enforcement review and investigative tracks. During their lifecycle, some SARs go directly to support investigations and some remain in the SAR database. A number of SARs that go into the SAR database will be used to support investigations at later times. Regardless of whether SARs are used to support investigations, they will be used in datamining initiatives to develop trend analysis or other strategic analyses.

Following my retirement from the FBI and as I have gained more of a financial institution perspective, based on my experience as a consultant, I have become more sensitive to the perceived lack of feedback to financial institutions from FinCEN and law enforcement regarding the value of SARs and how SARs should be written to get law enforcements attention. FinCen has done a good job of discussing the value of SARs in their SAR Activity Review publications. In recent years, FinCEN has recognized financial institution personnel as the frontend provider and law enforcement agents as the backend consumer for outstanding investigations involving BSA data.

When I was Chief of Financial Crimes, and subsequently TFOS, I had frequent meetings with Jim Sloan. During that time period, Mr. Sloan was Director of FinCEN. We often discussed developing a SAR feedback mechanism from law enforcement through FinCEN to financial institutions. There were many impediments that existed at the time, much as they continue to exist today, that precluded us from developing a consistent feedback mechanism. Some impediments include the ongoing nature and secrecy of federal grand jury investigations, the time lapse from when a SAR was filed and an investigation completed, resource constraints and other factors. Feedback regarding SARs warrants further consideration. This is an area where the Committee should consider dialogue with FinCEN and senior law enforcement executives.

The law enforcement utilization of SARs, as I have described how I used SARs as an FBI executive, was more at a program level than at the grass roots investigations level. At the program level there is a greater use of datamining and advanced analytics. At the grass roots field level, SARs are dealt with more in the form of individual manual reviews where each SAR is physically reviewed. For example, every U.S. Attorney's Office has a SAR review team. Even though the SAR review teams use excel spreadsheets and other analytics, they review SARs by hand. The reason this is important for the Committee is at the program level, I was more inclined to want to see more SARs filed. For our datamining purpose, more was better. At the grass roots level, SAR review teams would prefer to see less numbers of SARs filed. In this context, less is better. As a field agent and middle manager, I reviewed SARs manually, and I understand the grass roots perspective as well as the program perspective. Therefore, it is incumbent that as the Committee proceeds, you speak to a variety of law enforcement stakeholders to gain the best context available.

One final issue where law enforcement should be the primary stakeholder to potential legislation is the issue of CTR and SAR reporting thresholds. Since SARs were first implemented, the reporting thresholds have been the same. Periodically, banking associations and financial institutions have recommended that reporting thresholds be adjusted to account for inflation. I strongly believe that CTR and SAR reporting thresholds should remain as they are. Law enforcement would lose valuable financial intelligence if thresholds are raised. This is especially true for terrorist financing, where our primary threat is from homegrown violent extremists. My sense is that when we identify homegrown violent extremists and financial institutions run their names, a high percentage of them will have transactional activity involving CTRs.

As I've stated, at the core level, the flow of BSA data from the frontend provider (financial institutions) to the backend consumer (law enforcement) is good. When financial institutions can be proactive and more targeted in their monitoring and reporting, the BSA data they provide is more effective and efficient. When the data flow becomes convoluted and more constrained, the system becomes more flawed and ineffective and inefficient.

Thank you again for affording me the opportunity to testify today. I look forward to responding to any questions you have.



# Attachment



## Perspectives, Partnerships and Innovation

By Dennis M. Lormel

1/18/2011

I have been blessed throughout my 38-year professional career to be associated with truly outstanding professionals. I spent 31 years in government service, 28 with the Federal Bureau of Investigation. The integrity and dedication I encountered among my law enforcement peers was noteworthy. I was extremely proud of my friendships and associations. Over the last seven years as a consultant working with compliance and fraud specialists, I have had the privilege of observing the same levels of integrity and dedication. I have likewise been proud of the friendships and associations I've developed in the private sector.

The primary difference between my law enforcement and private sector colleagues is perspective. Not many people recognize this important fact. Both my law enforcement and private sector contemporaries understand the importance of partnering with each other. Unfortunately, successful partnerships have been on a one-off basis and not systemic and sustainable. One reason for this is the difference in perspectives.

Many of the individuals I have had the honor to associate with in law enforcement and the private sector are innovative thinkers. However, in most instances, they have been unable to affect institutional innovation. Law enforcement and private sector institutions tend to operate in their safety zones, and frequently, innovation falls outside the institutional safety zone. As a result, there is little incentive to develop innovative techniques to fight fraud and money laundering.

This brings me to the point of this article: perspectives, partnerships and innovation.

### Introduction

When it comes to fraud and money laundering, the bad guys are not constrained by boundaries. This affords them the opportunity to be proactive and imaginative in furtherance of their illicit activities. In fact, the more proactive and innovative the bad guys become, the more incentive they derive. Conversely, law enforcement and the financial services sector are frequently constrained by red tape and reluctance to implement change. Regulations, privacy considerations, policies, procedures, budgetary constraints and a myriad of other factors often serve as impediments to proactive measures and forward thinking. Regulations are such that reactive transaction monitoring and fraud detection in the financial services sector is the accepted norm. There is little incentive for innovation. Consequently, the bad guys have a considerable advantage.

As we've witnessed in the last few years, corporate frauds, investment frauds and mortgage frauds have devastated our economy. Add to that the continuous stream of check fraud, loan fraud and credit card fraud, not to mention health care fraud, and other crimes, and our economic problems are significantly compounded. The one constant in the various fraud schemes we have experienced is the ongoing need to launder these criminal proceeds. The intersection of fraud and money laundering should be the focal point for prevention and deterrence.

The time has come to take the advantage away from the bad guys in a sustainable and meaningful way. To achieve this, law enforcement and the financial services sector must first truly understand, embrace and act upon three words: perspectives, partnerships and innovation.

## **Perspectives**

In many of the training presentations I have given since I retired from the FBI, I have commented that when I retired and became a consultant, I thought I knew everything I needed to know about bank anti-money laundering (AML) and fraud compliance and investigations. What I came to realize in a heartbeat was how little I actually understood about the AML compliance and investigative function. It was not a matter of not knowing, it was a matter of not understanding the financial institution compliance and fraud perspective. That was a humbling and educational experience. Over the last seven years, I have worked hard to understand and appreciate the financial institution perspective. For the benefit of my law enforcement friends, if I knew then (when I was in law enforcement) what I know now, I would have been dangerous. I encourage my law enforcement colleagues to learn from my experience and look beyond your perspectives when dealing with the private sector.

The reality is that many law enforcement officers do not understand the perspective of the bank compliance or fraud specialist. Likewise, many bank compliance and fraud specialists do not understand the perspective of the law enforcement officer. The first step in progressing to sustainable and meaningful partnerships is for the two sides to understand and respect the differences in perspectives.

The fundamental difference in perspectives is that law enforcement is driven by criminal investigations. They must focus on developing evidence to support criminal prosecutions. Bank investigators focus on identifying and reporting suspicious activity. These two focuses would appear compatible; however, in between law enforcement and the banks sit the regulators. Without assessing blame to anyone, the regulatory system is such that the banks have to satisfy the regulators before supporting law enforcement. This is where the greatest strain on understanding perspective exists. Law enforcement is focused on their criminal case. They generally do not understand the banks' dilemma in having to satisfy regulators when there are bad guys to put in jail. In the meantime, banks are not necessarily concerned about whether the bad guys go to jail. They are concerned about getting the bad guys out of their banks and how the regulators will respond. Exacerbating the problem is the fact that although regulations and laws are written in black and white, their implementation and interpretation are gray and subjective.

Law enforcement and financial institutions need to address the conflict in their respective perspectives and understand that each possesses information that would greatly benefit the other. Law enforcement



has investigative and intelligence information regarding schemes and trends. I frequently hear complaints and frustrations expressed by bank compliance and investigative specialists that law enforcement does not share such information. Conversely, banks contain an incredible repository of financial information and intelligence that would greatly enhance criminal investigations if law enforcement was aware of its existence or where to obtain it.

Law enforcement and financial institutions must come to terms with perspectives. Once that is achieved, the foundation will be set for more productive partnerships. Such partnerships will be better positioned to be sustainable and meaningful.

## **Partnerships**

There have been a number of public and private partnerships that have achieved success. Most of these have been at the local or grass roots level. We need to develop more robust partnerships at both the grass roots and, more specifically, at the national level. The starting point should be with the realization that both law enforcement and financial institutions share the mutual responsibility to safeguard our financial system and their customers from fraud and money laundering.

One way to accomplish this is to develop crime problem specific partnerships. In doing so, law enforcement should develop case typologies specific to the crime problem and how the finances of the criminal activity flow through financial institutions. By sharing these case typologies and trend analysis information with the private sector, law enforcement will enable the private sector to more effectively and efficiently identify and report suspicious activity. By doing so, both sides benefit. Law enforcement develops evidence to support criminal prosecutions and/or, asset forfeiture and recovery. Financial institutions in turn will reduce institutional risk.

There is a great example of a public-private partnership that is crime problem specific and typologies driven. It was initiated by JPMorgan Chase (JPMC) under the leadership of William Langford. In 2009, JPMC Corporate AML founded a team dedicated to identifying and assessing immediate and strategic risks to JPMC. This outstanding team enthusiastically developed an issue-based approach by which they identified specific crime problems that presented them with significant risk. In 2010, JPMC identified human trafficking as a significant crime problem and a vehicle for institutional risk. Overall, the project developed typology-based surveillance models and investigator training to better enable the identification of potential human trafficking. JPMC's team of dedicated compliance and investigative professionals meticulously developed typologies which enabled them to identify transactional activity associated with human trafficking.

The next step was to develop active channels for coordination with relevant law enforcement agencies, especially those specifically focused on human trafficking. William and his team formed an outstanding working partnership with Immigration and Customs Enforcement (ICE), which has a dedicated group of agents assigned to investigate human trafficking. Through two way information sharing, JPMC was able to identify additional typologies while ICE was able to develop evidence to sustain criminal prosecutions.



Human trafficking is a heinous crime problem. The meaningful partnership formed by JPMC and ICE has begun to grow. In September 2010, during the annual ACAMS Conference, ACAMS executive vice president John Byrne hosted an informal, off the record, meeting between law enforcement and members of the ACAMS Advisory Board to discuss how ACAMS could facilitate partnerships between law enforcement and the financial services sector. Among some promising takeaways from that meeting came a subsequent meeting in Washington, D.C., between Byrne, advisory board chairman Rick Small, board member William Langford and senior executives at ICE. One of the topics was human trafficking.

Because of the devastating impact of this crime problem on its victims, ACAMS has formed a Human Trafficking Task Force, which Langford will chair. This initiative will provide a platform for the public-private partnership started by JPMC with ICE to grow and become more sustainable. In furtherance of this effort, on January 13, 2011, ACAMS hosted a free webinar training session on human trafficking. Byrne served as moderator along with ICE agent Angie Salazar, who provided a compelling training session. Education and training promote awareness, which frequently leads to action.

In establishing the issues based approach, JPMC did not settle for a traditional or reactive transaction monitoring framework. Langford and his team took an innovative and proactive approach to dealing with challenging crime problems. It should be noted that JPMC is not alone in developing innovative approaches to identifying and reporting suspicious activity. JPMC represents but one example of how certain financial institutions are gravitating toward the use of more proactive mechanisms.

## **Innovation**

Langford's team conducted extensive research to develop typologies. They relied on data mining and proactive targeted model development. By being proactive and focused, JPMC more effectively and efficiently identified suspicious activity consistent with human trafficking. The methodology developed by JPMC should serve as a model for future transaction monitoring models.

The industry needs to be less predictable in transactional monitoring and more targeted and proactive. There needs to be a balance between traditional reactive transaction monitoring and crime problem specific proactive targeted monitoring. A balanced approach between reactive and proactive monitoring would keep the bad guys off balance in their efforts to exploit areas of vulnerability.

A challenge going forward with this approach is incentive. The incentive for JPMC was doing the right thing. In terms of tangible incentives for financial institutions to implement similar typologies and methodologies, there is little. This is where the regulators could be a factor. If there was a regulatory incentive to develop crime problem specific monitoring typologies and proactive techniques, more financial institutions would be inclined to develop programs similar to JPMC's. This would significantly increase the generation of more consequential suspicious activity reports.

JPMC has applied the issues based approach to other significant crime problems. Hopefully, as they reach out to the relevant law enforcement agencies to form partnerships, those agencies will respond as



well as ICE did regarding human trafficking. Building meaningful and sustainable public-private partnerships is the best way to take the advantage away from the bad guys.

### **Conclusion**

Since the bad guys are not constrained by boundaries when it comes to fraud and money laundering, it is incumbent that law enforcement and the financial services sector share the responsibility to contain and disrupt criminal activity. The more proactive and coordinated law enforcement and industry are the more likely they are to deter the bad guys. The combination of perspectives, partnerships and innovation will provide the framework needed to stem the tide of fraud and money laundering.

