ACAMS US CAPITAL Chapter

U.S. Capital Chapter Winter 2022

Follow us: @acamsdc

Proliferation Financing:
Tackling the Risks, Threats and Challenges
Rachele Byrne

On July 26th, the U.S. Capital Chapter held a virtual learning event on the risks, threats, and challenges of proliferation financing. The event was moderated by Lauren Kohr, Senior Director of AML-Americas at ACAMS and board member of the U.S. Capital Chapter, and featured three proliferation financing subject matter expert panelists from both the private and public sectors: Dr. Jonathan Brewer - Visiting Professor, King's College, London; Neil Bhatiya - Policy Advisor, Office of Terrorist Financing and Financial Crimes, U.S. Department of the Treasury; and Barbara Ditoto - Program Manager, FBI WMDD.

Ms. Kohr began the event by introducing the panelists and setting the tone for the discussion, stating that the topic was a timely one as FinCEN had just published its first national AML/CFT Priorities in June, which included proliferation financing on the list. Dr. Brewer then started the dialogue by providing an overview of how proliferation financing has been defined and viewed by the international community in the past. He stated that, historically, government and law enforcement regarded the proliferation financing threat as lower than that of money laundering. However, this thinking has changed in recent years as evidenced most recently by the Financial Action Task Force's (FATF) modification in October 2020 of its 40 Recommendations to include proliferation financing within the scope of the first recommendation on risk assessments. Dr. Brewer noted that proliferation financing, can include both in-country manufacturing of weapons of mass destruction and the procurement of related goods or materials. In-country manufacturing is typically financed by state government budgets. The procurement of goods and or materials is sourced from countries overseas. On a global scale, proliferation financing is hard to measure. Dr. Brewer gave one example, stating that FinCEN estimates that millions of U.S. dollars of North Korean illicit activity have flowed through U.S. correspondent accounts. With the recent changes made by FATF, financial institutions need to start incorporating proliferation financing into their risk assessments. Dr. Brewer stated that in-country manufacturing should be thought of in relation to correspondent banking accounts while procurement activities might be identified in relation to trade finance products and services. He noted that while financial institutions primarily leverage sanctions controls to address proliferation financing risk, they will have to do more in the future to manage the risk in this space.

Barbara Ditoto from the FBI then provided an overview of U.S. law enforcement's view of proliferation financing. She defined proliferation financing from a U.S. law enforcement perspective, drawing a distinction between it and terrorist financing. While terrorist financing is usually self-funded, proliferation financing is funded by state actors who provide the funding via front and shell companies, allowing the transactions to hide in plain sight. She also noted that, while proliferation financing is not a predicate offense, sanctions and financial crimes regulation (i.e., money laundering, bank fraud) can be applicable and used to prosecute. Ms. Ditoto then reviewed the Department of Justice (DOJ) Export Enforcement Report, stating that it can be used by the private sector to pull out analysis of trends that law enforcement is seeing in this space to

Note from Chapter Co-Chairs
Dennis Lormel & Sepideh Rowland

With 2021 in the rear-view mirror, we take a moment to reflect back on last year and the emerging risks in financial crimes. The U.S. Capital Chapter has continued to deliver virtual events focused on these emerging risks, such as ransomware and proliferation financing. The world has changed over the last year, whether that is adoption of digital payments and cryptocurrencies or the shift on the global stage with heightened risks posed by Russia and China, along with the Taliban takeover of Afghanistan. In September, we took time to reflect upon the 20th anniversary of 9/11 to recognize the significant progress made in combatting illicit finance and acknowledge the work that lies ahead.

We will continue to deliver virtual events in the coming year until such time that it is safe for us to meet again in person.

If you are interested in volunteering for the Program Committee or the Chapter's Advisory Board, please contact us. You can reach us either through LinkedIn or via email at USCapitalChapter@acams.org.

Tentative upcoming Event Topics in 2022:
January – Sports betting
February – GAO Trafficking & Trade Based Money Laundering Reports
March – Corruption & Bribery

Please visit our website for up-to-date information: http://www.acams.org/acams-chapters/u-s-capital/#events

Our Board Members:
Dennis Lormel (Co-Chair), Sepideh Rowland (Co-Chair & Editor), Kevin Anderson (Treasurer), Barbara Keller (Program Director), Bob Pasley (Communications Director), Rachele Byrne (Social Media Director), Lauren Kohr (Membership Director)
Members at Large: Don Temple, Ed Rodriguez, Lester Joseph, Steve Gurdak, and John Wagner.

help aid them in monitoring their own institutions for similar activity. She provided analysis based on the most recent publicly available reports, reviewing the technology and country trend summary from the DOJ export enforcement cases. Iran continues to be the leading country involved in the export enforcement cases the DOJ is reporting as Iran continues to seek U.S. technology in the proliferation financing space, as they have for several decades. Technology of concern from these cases include advanced military technologies (i.e., carbon fiber, night vision goggles, military grade tech, laboratory equipment, and/or source codes); electronic devices (i.e., IED components; controlled micro-electronics; and space communication technology); and aviation (i.e., aircraft components; turbine technology; and unmanned aerial vehicles); among others. Ms. Ditoto concluded by reviewing best practices for financial institutions monitoring and reporting this type of activity, including ensuring they provide detailed personal information, country affiliation, the technology or material sought by the country or person, and/or the shell/front company information in any filed SARs or STRs.

Neil Bhatiya from the Treasury Department then provided an overview of how the U.S. government is assessing and mitigating the risk of proliferation financing. He noted that, as Dr. Brewer alluded to in his opening remarks, FATF published guidance on proliferation financing for jurisdictions and financial situations, which included best practices for incorporating it into risk assessments going forward. While the current risk assessments performed by both the private and public sectors typically only apply to sanctions targets, it is recommended that the scope be widened as sanctioned governments, entities, and persons are not the only actors in the area of proliferation finances. The FATF guidance also addresses de-risking and sets supervisory expectations in this space. Along those lines, Mr. Bhatiya stated that the U.S. Treasury is currently working on updating its national proliferation financing risk assessment.

Dr. Brewer concluded the virtual learning session by reviewing some recent proliferation financing case studies and providing some best practice recommendations for financial institutions that are working to improve their control framework. He noted that, while proliferation financing typologies have not changed much in the last 10-15 years, recent reports published by the U.N. Panel on North Korea have cited an increased use of cyber-attacks to raise funds for government activities. While there is no public reporting available on the use of cyber-attack funds for proliferation financing specifically, it makes sense that they could be used for such activities in the future. In terms of financial institutions, Dr. Brewer emphasized the importance of customer due diligence, particularly for any financial institutions that are involved in trade finance. Institutions should continue to share information amongst themselves and with law enforcement to ensure both the private and public sectors are best equipped to fight this threat.

9/11: Twenty Years Later

Barbara I. Keller, CAMS

On September 10th, the day before the twentieth anniversary of the 9/11 terrorist attacks, U.S. Capital Chapter members had the unique opportunity to hear from some of the architects of war on terrorism that focused on terrorist financing. The session was moderated by chapter co-chair, Dennis Lormel, who was the head of Financial Crime Programs at the FBI in 2001. David Aufhauser was the Treasury General Counsel and William Langford was his senior advisor. Together, Treasury and the FBI developed our approach to tracking potential funding for terrorist attacks. The session traced the history of our counter-terrorist financing efforts from 9/11 until today.

Prior to 9/11, there was no focus on terrorist financing in the U.S.—that changed drastically after 9/11. Mr. Aufhauser commented that they were "stunned, slack-jawed, and embarrassed" after 9/11 – no one had a clue about how the money for the attacks got into the system. Mr. Lormel commented that the terrorists had between $400,000 and $500,000; $328,000 of which came through the financial system. The White House placed the effort to tackle terrorists and terrorist financing under the National Security Council – this was a seminal development. Treasury was put in charge of the financial side of the effort. Mr. Aufhauser created the Policy Coordinating Committee on Terrorist Financing (PCC) at the interagency level and approached Mr. Lormel to join forces with law enforcement and to begin outreach to the financial sector. This was truly the first public-private partnership - everyone wanted to help.

Mr. Langford commented that many elements of the programs and regulations put in place post-9/11 were already under development. 9/11 galvanized the efforts to pass what became Title III of the USA PATRIOT Act. 9/11 was also transformational for the Financial Action Task Force (FATF) - it solidified the link between money laundering and terrorist financing. FATF quickly developed and issued the Special Recommendations on terrorist financing, which were eventually incorporated into the 40 Recommendations.

Mr. Aufhauser explained the Treasury's relationship with SWIFT[1] in the aftermath of 9/11 to try to track financial transaction data that might be useful to prevent future terrorist attacks. This program was conducted in secret for three years until it was the subject of a New York Times exposé. Shortly after 9/11, Mr. Aufhauser reached an agreement with SWIFT to provide U.S. authorities with certain limited-scope transaction data. Strict protocols were placed around the process and its security. Through tracing transactions, this data enabled the authorities to identify networks of people and disrupt acts of terror. The information identified through analysis of the SWIFT transaction data formed the basis of the weekly PCC meetings until 2006 when the New York Times blew the cover on the relationship. This relationship between the U.S. government and SWIFT was the first true public-private partnership on terrorist financing.

Mr. Lormel explained that, once they knew who the hijackers were, law enforcement built a financial chronology on all of them. They identified credit cards, bank accounts, wire transfers, etc. They were able to establish the entirety of the funding flow within a few weeks. It's not clear if the hijackers used hawalas but they did use bulk cash and travelers checks. Law enforcement was able to trace the money back to Osama Bin Laden. Mr. Aufhauser explained that the information developed by the FBI, confirmed how central the banking system was to stopping terrorist financing. He was surprised at how much the banking system had been exploited. This affirmed the need for the government's partnership with banks and reinforced Treasury's initiatives that evidence and important intelligence could be found in the banking system. Going forward we can use financial intelligence proactively.

In response to a question about how to proceed on Afghanistan, Mr. Aufhauser commented that it was "back to the future." Law enforcement will have to up its game again to try to stop money flowing to jihadist groups and find ways to develop intelligence on the money flows. Mr. Langford commented that, unlike 20 years ago, banks have a better idea of their global exposure. They know their products and services better. There are avenues for law enforcement and the intelligence community to reach out and collaborate to help everyone understand what's happening. We are better positioned, but we won't know everything. Financial institutions know their clients and their clients' activity, but they need to find out what else they need to look for and ferret out indirect exposure.

Is the financial system a facilitation tool or a detection mechanism? In 9/11, there was nothing suspicious in the transactions – the hijackers weren't even discrete, which made it easier to trace the financial flows after the fact. The final takeaway from the discussion is that collaboration between government agencies and public private partnerships is essential in combatting terrorist financing.

Money Laundering and Real Estate

Bob Pasley

On October 19th, the U.S. Capital Chapter of ACAMS hosted a webinar on money laundering and real estate. The moderator was Barbara Keller, a board member of the Chapter. The presenters were Lakshmi Kumar, the Policy Director for Global Financial Integrity (GFI); Les Joseph, a board member of the Chapter and the Manager of Wells Fargo's Global Financial Crimes Intelligence Group; and Michael Sallah, the Senior Investigations Editor for the Pittsburgh Post Gazette.

The webinar focused on the recently issued GFI report entitled "Acres of Money Laundering: Why U.S. Real Estate is a Kleptocrat's Dream." Ms. Kumar, the principal author of the report, explained that the report dives into the murky world of global money laundering and demonstrates the ease with which kleptocrats, criminals, sanctions evaders, and corrupt government officials choose the U.S. real estate market as their preferred destination to hide and launder proceeds from illicit activities.

Ms. Kumar began by speaking about Geographic Targeting Orders (GTOs), which FinCEN has been using since 2016 to try to track residential real estate transactions that do not involve a mortgage through a financial institution. The initial GTOs only covered Manhattan and Miami-Dade County and covered transactions between $1 and 3 million. Since then, the GTOs have been renewed 10

[1] The Society for Worldwide Interbank Financial Telecommunication (SWIFT), legally S.W.I.F.T. SCRL, provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment.

times, expanded to cover 22 different counties, and the dollar amount has been reduced from $1-3 million (depending on location) to $300,000 in order to cover more transactions. One of the limitations of the GTOs, however, is that they are restricted to residential real estate and to cases where the property is purchased by a legal entity with "all cash," including cash, money orders, checks, wire transfers, and virtual currency.

In their study, GFI reviewed 56 different public cases involving the laundering of $2.3 billion through the use of real estate. In many of these cases, gatekeepers (including attorneys, real estate agents and brokers, and investment advisors) played an integral part in the transactions, but were not subject to AML requirements – unlike all of the other G-7 countries. Lawyers were involved in 36% of the cases and real estate agents and brokers were involved in 25% of the cases.

In addition, GFI found that 82% of the cases involved money coming from 26 different foreign countries, 50% of which were in Latin America. Also, the majority of the cases involved "politically exposed persons" (PEPs), likely using the proceeds of corruption. Ms. Kumar commented that this is disconcerting given the fact that the U.S. supports many of these countries with financial aid.

In the case of Equatorial Guinea, its President, Theodoro Obiang, bought 127 properties in Florida, mostly through lawyers and using "Interest on Lawyers' Trust Accounts" (IOLTAs). In addition, the Venezuelan government invested money in Florida real estate.

In 60% of the cases GFI reviewed, there were no GTOs in effect due to the limited geographic coverage of GTOs. In addition, 30% of cases pertaining to real estate-based money laundering involved commercial real estate. These facts demonstrate some of the shortcomings of GTOs.

Michael Sallah discussed his reporting on Ukrainian oligarch Igor Kolomoisky for various news organizations, including the International Consortium of Investigative Journalists and the Pittsburgh Post-Gazette.

Kolomoisky and his associates purchased 22 properties valued at nearly $1 billion, including 13 steel factories, five office towers, and two office parks, mostly in small towns so he avoided the scope of GTOs which did not cover these towns, and, as noted above, and focused only on residential real estate. Many of the properties were not purchased for long-term investment, but rather were run into the ground, resulting in bankruptcies and lost jobs. There were various red flags, including OSHA violations; the inability of Kolomoisky, the owner of the steel factory, to obtain a U.S. visa; no audited financial statements; and suspicious activity reports filed by Deutsche Bank, the financial institution moving the money into the United States from Ukraine and Cyprus. Local governments raised red flags, but there was little due diligence for various loans – in fact, the City of Cleveland gave the factory $43 million in economic development loans. The DOJ investigation took 10 years, but a Grand Jury in Ohio is now looking into the case and there are several civil lawsuits.

A Ukrainian bank, PrivatBank, sent at least $1 billion on Kolomoisky's behalf to the U.S, mostly through offshore bank accounts registered in Cyprus and the British Virgin Islands. Eventually, Ukraine determined that fraud was involved and nationalized the bank. Kolomoisky's bank also assisted Kolomoisky and moved hundreds of millions of dollars for him from Ukraine to the U.S. The bank found his activities suspicious and filed Suspicious Activity Reports, but did not stop his transactions.

Law Enforcement Corner
Dennis M. Lormel

A constant theme the Advisory Board of the U.S. Capital Chapter has stressed is the importance of public-private partnerships. The more we can do to promote information sharing, help build a common understanding of financial crimes, and bring together perspectives of all AML stakeholders, the more we will learn of ways to disrupt the illicit flow of funds and deter criminal activity.

FATF has urged law enforcement to charge suspects of money laundering with all appropriate predicate offenses. Taking that guidance a step further, FATF has recommended that law enforcement conduct financial investigations as a component of all criminal investigations. The critical information necessary for law enforcement to conduct such financial investigations and connect the dots resides with the financial institutions. The key to success is to have law enforcement investigators *"understand"* how they can benefit from financial institutions and, conversely, for financial institution investigators to *"understand"* how they can benefit from law enforcement.

This makes information sharing that much more important and our Chapter's focus on public-private partnerships more meaningful. Through our programming and outreach efforts, our Chapter strives to provide a pathway to enhance *"understanding."* By doing so, we strengthen the common thread between law enforcement and financial institutions. In that regard, we welcome all suggestions from our members to continue to provide the quality programming that fosters "understanding."

Les Joseph reiterated the fact more than 80% of real estate-based money laundering emanates from overseas and pointed out the fact that it is the gatekeepers – the attorneys, the real estate brokers and agents and title companies – who know these individuals the best. Banks, in contrast, are mostly in the position of accepting wires that go to large law firms and realtor firms. These entities are known to the bank, but the underlying individuals are not. Mr. Joseph pointed out the fact that, unlike banks, attorneys and realtors do not participate in the §314(b) information sharing process of the USA PATRIOT Act, thus making it difficult to obtain information about the transactions. He further noted that, if a bank were to question a transaction from a law firm, the response from the law firm would probably be that providing any information would breach client confidentiality rules.

Private-Public Sector Partnership

While it may be true that there are more SARs than there are agents and officers to always look into each one, there are times that should not be the case. Whether it is just a hunch, a coincidence, or "just doesn't look right" and you believe a particular SAR deserves to be looked at, don't forget about the U.S. Attorney's Office for the Eastern District of Virginia's (EDVA) special ***SAR tip email line @ "usavae.sars@usdoj.gov***."

Your tip (SAR) can stay anonymous or confidential, but rest assure someone will take a look at it.

Mr. Joseph also pointed out the fact that gatekeepers are the weak link in the U.S. AML regime. For example, while the BSA's definition of "financial institution" includes "persons involved in real estate closings and settlements," they have been exempted by FinCEN from BSA coverage. Panelists noted that the lobbying arms of many types of gatekeepers are extremely strong and, so far, have effectively argued against being covered by AML requirements. They said that things like the publication of the Panama Papers and the Pandora Papers can tend to diminish the strength of this lobbying effort. The ENABLERS Act was introduced in the wake of the release of the Pandora Papers. It aims to close loopholes that kleptocrats use to launder money in the U.S. It would eliminate the exemptions currently in place and would also require that Treasury create due diligence rules on source of funds for investment advisors, art dealers, and attorneys, among others. Mr. Sallah commented that, if passed, it would help to provide a balance between regulation (compliance with AML) and business (profit).

In closing, some of the panel's recommendations included the passage of the ENABLERS Act, the expansion of GTOs to be nationwide and to include commercial real estate, the creation of a nationwide standard for the establishment of corporations, and prioritization of implementation of the beneficial ownership registry.

Ransomware is Everywhere: Tracing Payments to Fight a National Security Threat

Barbara I. Keller, CAMS

On November 9th, the U.S. Capital Chapter hosted a virtual discussion of the national security threat posed by ransomware. Ransomware attacks are increasing and getting more sophisticated. Moderator Les Joseph, Chapter Board member and Manager of Global Financial Crimes Intelligence at Wells Fargo, led the conversation with panelists Mike Caswell, Special Agent, U.S. Secret Service; and Chad Ratashak, Financial Crimes Associate of Global Financial Crimes Intelligence Group at Wells Fargo. Organizations need to not only do everything they can to protect themselves, but also know what to do if they are the subject of an attack. Prevention and mitigation are key. There are a number of best practices to follow – patching hardware and software, restoring, and rebuilding once the system goes down.

Financial institutions are in the position of being both potential victims of ransomware attacks as well as possible facilitators of ransomware payments. As possible facilitators, banks have to be aware of the risks of possibly facilitating a ransom payment. For example, ransomware was mentioned in OFAC's September 2021 Advisory. In that advisory, OFAC highlighted the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities, and discussed the proactive steps companies can take to mitigate such risks. The advisory recommends measures such as offline backups of data, developing Incident response plans, cybersecurity training, updating anti-virus and anti-malware software, and authentication protocols. The advisory further recommends siloing information on a need-to-know basis. This will help limit the damage from an attack. Mr. Ratashak explained that threat mitigation and sanctions risk go hand-in-hand. OFAC will look at your mitigation measures if a possible sanctions violation may occur. OFAC will consider whether the company had taken precautions and whether it did everything it could have. OFAC considers reporting an attack to law enforcement to be a voluntary self-disclosure for sanctions purposes.

Mr. Caswell said that spear phishing attacks are still prevalent and cautioned attendees to be careful what you click on. Security training is essential due to the high volume of attacks. Incidence response is key – companies need to have a plan in place, test their

systems, and know who to call and how to respond if attacked. He recommended that companies perform mock exercises to test and be familiar with their protocols. In addition, companies need to establish and maintain standing relationships with law enforcement and their regulators. The US Secret Service has 44 cyber-fraud task forces globally. The FBI also has its own task forces, and the Secret Service and FBI do a lot of information sharing. There is a "Preparing for a Cyber Incident" part of the Secret Service's webpage.

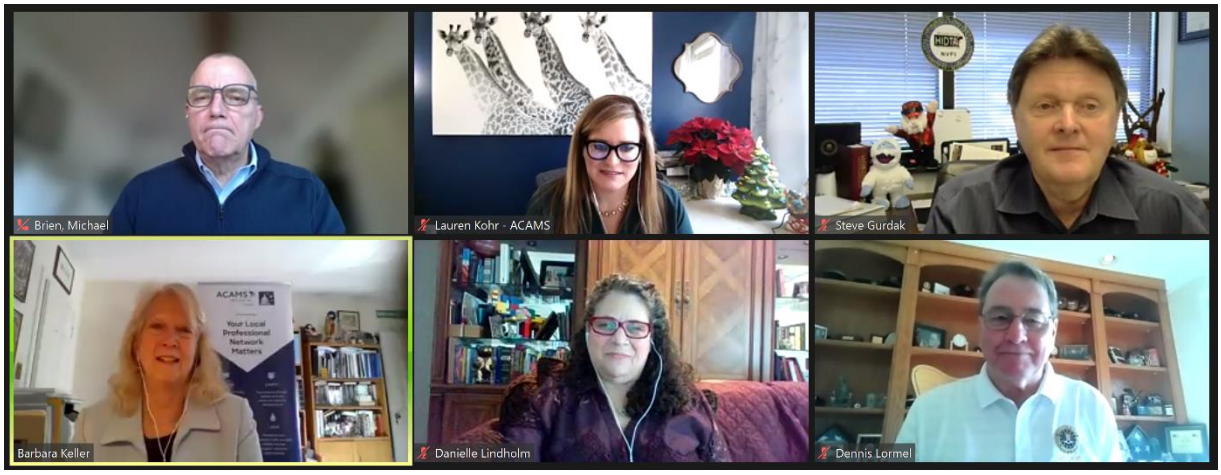
FinCEN issued a ransomware advisory in 2020 and an updated ransomware advisory on November 8, 2021; the changes reflect a greater focus on the dollar side of ransomware payments, including the role of depository institutions, digital forensics, and incident response (DFIR) companies, and cyber insurance companies (CICs). FinCEN wants financial institutions to report ransom-related payments in SARs, which Mr. Ratashak explained may include depository institutions' customers sending payments to DFIRs or CICs. He explained that this is not because DFIRs or CICs are criminal, or that paying a ransom is a crime (although paying specific entities may violate sanctions), but the activity may nevertheless be suspicious because it is related to the facilitation of a ransom payment. Financial institutions are in the middle of the situation and may have greater visibility on ransom-related payments than they realize, even if they have little to no direct exposure to cryptocurrency. This visibility may come through depository institutions' customers that become victims of ransomware or customers that act as ransomware intermediaries, like DFIRs and CICs. He explained that promptly identifying these ransom-related payments helps law enforcement follow the money to identify cybercriminals.

FinCEN wants financial institutions to be aware of their reporting responsibility, whether or not they are paying the final cryptocurrency ransom. Mr. Joseph explained that FinCEN is likely looking at SARs filed by intermediaries, such as DFIRs, and trying to match them up with what depository institutions and others are reporting. FinCEN is trying to ensure that all possible ransomware payments are properly reported so that law enforcement can get a comprehensive view of the scope of the ransomware problem.

Year in Review and Predictions for 2022
Bob Pasley

On December 15th, the U.S. Capital Chapter held its annual Year-in-Review. The webinar was moderated by U.S. Capital Chapter Board member Barbara Keller. Panelists were Danielle Camner-Lindholm, Director of National Security Policy, House Financial Services Committee, Lauren Kohr, Senior Director of AML-Americas at ACAMS and board member of the U.S. Capital Chapter, Michael Brien, Managing Director of Risk & Financial Advisory at Deloitte, Steve Gurdak, Group Supervisor, Northern Virginia Financial Initiative, Washington/Baltimore HIDTA and a board member of the U.S. Capital Chapter, and Dennis Lormel, President of DML Associates and U.S. Capital Chapter co-chair.

The panelists discussed the Anti-Money Laundering and Corporate Transparency Acts, which were passed as part of the National Defense Authorization Act of 2020, and several of the recent FinCEN rulemakings including the Notice of Proposed Rulemaking on beneficial ownership.



Ms. Camner-Lindholm discussed some of the hearings held before the House Financial Services Committee, including those related to the financing of domestic terrorism, human trafficking, and wildlife trafficking. She indicated that, going forward, the Committee will follow up on studies required by the AMLA, including, among other topics de-risking; trade-based money laundering; trafficking; the dark web; sanctions; corruption; and cyber financial crime. She also expects a hearing focused on FinCEN's progress in

implementing its taskings in the AMLA and CTA. The Committee will look to expanding special measures and explore virtual assets and possibly Central Bank Digital Currency.

Ms. Kohr focused on issues from the perspective of financial institutions, including the issue of how to make AML programs and the work of financial institutions more effective. She also discussed the need for rulemaking to consider the perspective of financial institutions and how financial institutions can provide useful information to law enforcement. In addition, she stressed the need for more private-public coordination at all levels.

Mr. Brien addressed various issues from the viewpoint of consultants that work with financial institutions, including data testing and model validation, and the risks that can be identified through these processes. He also noted that the work-from-home regiment dictated by the pandemic has not resulted in the material data breaches that were feared. He expects most institutions will have more employees working from home, at least part of the time, in the future.

Mr. Gurdak discussed the framework of the three SAR review teams located in the D.C., Virginia, and Maryland metropolitan area. He reviewed the macro and micro issues related to SARs and the areas they cover, including ransomware and cryptocurrency. He also noted that some large cases have their origin with small or modest SARs. He is a big proponent of using the BSA in a different way – there is a financial component to most crimes and so he believes SARs should be mined for financial transaction information that can strengthen law enforcement cases. SARs can also help to identify additional suspects. He commented that, from his perspective, the big emerging issue is the fentanyl pandemic and the resulting level of overdoses.

Mr. Lormel reviewed the existence of COVID-related frauds and the nature of terrorist threats, which now include individually driven and domestic threats, culminating in such events as the January 6th insurrection. However, in his view, we might see less domestic terrorism going forward due to the indictments and convictions against many of those involved in the January 6th riot and the various civil suits that have been filed, including one recently filed by the DC Attorney General against the Proud Boys and the Oath Keepers. He noted that some issues he expects we will see going forward include virtual currency fraud, including fraud through virtual currency investment schemes; and elder fraud, which has been a problem for over 20 years.

Thank you to our speakers: David Aufhauser, Neil Bhatiya , Dr. Jonathan Brewer, Michael Brien, Mike Caswell, Barbara Ditoto, Steve Gurdak, Les Joseph, Barbara Keller, Lauren Kohr, Lakshmi Kumar, William Langford, Danielle Camner Lindholm, Dennis Lormel, Chad Ratashak, and Michael Sallah.