



Recent Financial Crime Trends: Organized Retail Crime and Cybercrime

Barbara I. Keller, CAMS

On June 23rd the U.S. Capital Chapter was pleased to host a webinar focused on recent financial crime trends presented by two law enforcement agents. The program was moderated by Chapter Board member Don Temple, with speakers Jonathan Helmstetter, Supervisory Special Agent IRS-Criminal Investigations who discussed cybercrime trends and Johnathan Willis, Special Agent U.S. Department of Homeland Security Investigations who discussed organized retail crime.

Mr. Helmstetter began by providing an overview of the work of IRS-CI and its role in investigating financial crime as the only federal law enforcement agency with jurisdiction over violations of federal tax laws and it shares jurisdiction over money laundering and BSA. IRS-CI is involved in cybercrimes investigations where it has both investigative authority and the subject of the investigation is believed to be committing a tax or other financial crime while using the internet as an essential means to commit the crime, remain anonymous, elude law enforcement and/or to conceal financial transactions, ownership of assets, or other evidence.

He explained that there are two types of cybercrime:

- **Cyber-enabled** – These crimes are more traditional in nature, which can only be increased in their scale by the use of computers, computer network or other form of communications technology. These crimes include theft and fraud of all types.
- **Cyber-dependent** – These crimes can only be committed using a computer, computer network or other form of communications technology. Simply, if not for the internet, these crimes would not exist. These crimes include hacking, viruses, and Distributed Denial of Service (DDoS) attacks.

IRS-CI's primary focus currently is tax evasion through the use of virtual currency. Cryptocurrency is becoming more mainstream for laundering money and the cryptocurrency portion of seizures is increasing each year.

Mr. Helmstetter walked through some of the examples of how crypto and the dark web are involved in cybercrimes to facilitate money laundering or fraudulent activity. He provided an overview of the development and evolution of the Cyber Unit, which was developed in 2014 as a result of the Silk Road investigations. IRS-CI has agents who are exclusively devoted to online monitoring.

He explained the difference between virtual and cryptocurrency. Virtual currency is defined as a digital representation of value that is neither issued by a central bank (or a public authority), nor necessarily attached to a fiat

Follow us:



@acamsdc

Note from Chapter Co-Chairs

Dennis Lormel & Sepideh Rowland

The second half of this year showed the renewed enthusiasm of our Chapter members coming back to in-person events. We launched our first in-person event with the Fourth Annual Public-Private Sector Partnership Forum where we had all of the federal law enforcement agencies represented and 175 attendees, demonstrating the importance of collaboration and partnership. This event was followed by another in-person event focused on Human Trafficking and a moving presentation by Matt Friedman on his first-hand experiences in fighting human trafficking in Asia.

We also continued our virtual program focused on emerging risks and hot topics facing financial crimes compliance professionals.

We are once again assembling our Program Committee to provide the Board support with program development and coordination of in-person events. If you are interested in joining the Program Committee or the Chapter's Board, please contact us. You can reach us either through LinkedIn or via email at USCapitalChapter@acams.org.

Tentative upcoming Event Topics in 2023:

January – Personal Liability

March – American Kingpin: The Dark Web

April – Crypto Forum (In-person)

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, John Wagner, and Ray Villanueva.



currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically. A cryptocurrency is a digital currency using cryptography to secure transactions and to control the creation of new currency units. Currently, there are over 10,972 cryptocurrencies in circulation with a market value of approximately \$1.3T and 382 exchanges. Every single transaction conducted in digital currency is tracked on the ledger. IRS treats digital currency as assets and sees these transactions similar to stock trading.

Mr. Helmstetter outlined three different types of crypto-related activity that can be attributed to targets of investigations:

- On ramps: customer opens an account at a crypto exchange or a business that accepts payment in cryptocurrency.
- Off ramps: customer “cashes in” the crypto through the exchange or purchases goods online or at a store. This can also be done through Bitcoin ATMs and peer-to-peer exchanges.
- Clustering: takes one address you have attributed to your target and expands the area to estimate other address also controlled by your target. Third party software is used for this analysis.

The first cryptocurrency case was Liberty Reserve, a digital currency exchange, in 2013. The largest cryptocurrency seizure ever was \$3.6 billion in the Bitfinex hack in 2016. In all of these types of investigations, IRS-CI was the lead agency in the cryptocurrency tracing and ultimately the attribution of main targets or the associated network servers. In addition, IRS-CI participates in many joint agency cyber task forces which include other local, state and federal law enforcement agencies.

Mr. Willis discussed organized retail crime (ORC), which is a relatively new emerging issue. There are many reasons why the federal government is getting into fighting it as this type of crime can't be fought only at the state level. There are networks of organized crime rings that participate in retail crimes, including smash and grabs. These criminal organizations, which comprise individuals with no legitimate income who fence these stolen items for cash as a source of income, having a detrimental impact on the retailers. In most cases, they try to stay non-violent to keep law enforcement less interested. Mr. Willis outlined several lessons learned from recent cases that should be used in continuing to fight ORC:

- value of partnerships,
- collection of evidence,
- organization,
- buy in from leadership,
- quality of work, and
- manpower demand.

Mr. Willis said that the financial indicators of ORC that banks should be on the lookout for are often similar to red flags presented for money services businesses and migrants.

Corruption and Kleptocracy: Two Sides of the Same Coin?

Barbara I. Keller, CAMS

As part of its 2022 series on corruption, the U.S. Capital Chapter was pleased to hear from Debra LaPrevotte, senior investigator with The Sentry, on August 15th, moderated by Chapter Co-Chair Dennis Lormel. Ms. LaPrevotte discussed kleptocracy and corruption and how they are sometimes two sides of the same coin. She began her presentation by providing some background on corruption and laying the foundation for how this impacts the daily lives of the citizens of the countries that have a higher propensity for corruption. She reviewed the common characteristics of kleptocracy and how kleptocrat leaders often use their power and influence to take over lucrative industries, businesses and media in order to enrich themselves and stay in power.

She highlighted that Africa has a high proportion of the world's worst kleptocrat states, listing out the most egregious individuals who have been in office, their association with alleged corrupt practices, and their net worth. She demonstrated through examples that these individuals amassed significant personal wealth during their reign of power. Another issue often related to kleptocracy is corruption is looting of natural resources. The corrupt networks used to transfer these both the illicitly gotten natural resources and sales proceeds are often the same networks used to move



money and evade sanctions in jurisdictions like the U.S. Ms. LaPrevotte noted that these countries should be thriving from the use of these natural resources but they are not, and the profits from the natural resources are not benefiting the citizens of the country, many of whom continue to live under poverty standards. The Sentry explored the poverty level and health and social programs, which showed that the benefits of these natural resource-rich countries were not cascading down to their people.

Studies show that in the U.S., 12% of adults are illiterate, compared to other countries like Afghanistan where 62% are illiterate or South Sudan where 85% of females are illiterate and 63% of males are illiterate. Studies also showed that in these countries there is also a high infant mortality rate. Non-governmental Organizations (NGOs) are often involved in these countries to provide medical and food support.

Another common characteristic of kleptocrats is the suppression of media and repression of journalists and activists. Often news footage obtained by media outlets is destroyed and witnesses are killed to suppress information the kleptocratic regime does not want released.

Ms. LaPrevotte detailed some of the investigative cases she focused on during her tenure with the Federal Bureau of Investigation (FBI) in South Sudan where elections were recently postponed for two years. She noted that kleptocratic regimes almost always have an interest in industries related to petroleum, banking, mining, and minerals which often also involve employment of immediate family members to be a part of the companies and as a way to mask the corrupt practices. An example of this is the former Ukrainian Prime Minister Lazarenko, who was indicted in the U.S. on 59 counts related to money laundering in 2006. He was convicted and served nine years in prison. Through her work at The Sentry, Ms. LaPrevotte noted that she conducted a review of the children of kleptocrats which demonstrated how wealthy they are and how they benefit from the leadership roles of their parent. These family members often purchase luxury items that have been subject to seizures when they are later identified to be from the proceeds of corruption.



Kleptocrats have also been off-shoring wealth into countries seen as havens or secrecy jurisdictions, such as Dubai, Nauru, Vanuatu, U.S., Cyprus, British Virgin Islands, Isle of Man, Kenya, and Uganda. They are attractive because they offer “enablers,” such as financial institutions, that have been discovered to be sheltering the corrupt funds. There are also attorneys, incorporation service providers, and jewelers/art/antiquities dealers that have been identified as enablers.

Finally, Ms. LaPrevotte described the U.S. federal law enforcement’s response to kleptocracy, including the dedicated Foreign Corrupt Practices Act and Recovery (FCPA) unit within the U.S. Department of Justice, and International Corruption units of both the FBI and the United Kingdom’s National Crime Agency. In addition, NGOs and investigative journalist play a big role in helping to identify corruption.

Fourth Annual Public-Private Sector Partnership Forum

Barbara I. Keller, CAMS

On September 29th the U.S. Capital Chapter was pleased to hold its Fourth Annual Public-Private Partnership Forum in-person. ACAMS President Scott Liles offered the welcome remarks to attendees. Attendees heard from more than 20 speakers from federal and state law enforcement agencies. The event began with a keynote from FinCEN; then special presentations from the FBI’s Counterterrorism Division, IRS-CI, HSI’s Transnational Organized Crime Division, and three panel discussions – Public-Private Sector Partnerships in the Beltway, Emerging Fraud Trends and Red Flags, and Understanding Financial Flows of Fentanyl and Illicit Drugs.



The bottom-line message to the audience from the law enforcement agency representatives in the first panel was that the importance of public-private partnerships has grown over the years and the relationship has gotten better. The key takeaway from IRS-CI is that criminals are opportunistic and take advantage of any opportunities. A lot of the data provided in SARs are only the tip of the iceberg. Sometimes looking at suspicious activity reports (SARs) is like looking for a needle in a stack of needles. The data doesn't provide sufficient context, but that's where law enforcement comes in – law enforcement has the context. This is why the relationship is crucial. The Assistant U.S. Attorney for the Eastern District of Virginia has created a SAR tipline for banks to use to reach out to his office and flag cases that require more immediate attention and review in an effort to pinpoint the most critical needles.



The FBI Deputy Assistant Director for Terrorism said that countering terrorism is FBI Director Wray's number one priority. The terrorism threat has evolved and state-sponsored terrorism and domestic terrorism have both become problems. The FBI discusses partnerships in all their meetings as a way to help mitigate and disrupt threats.

The emerging fraud trends panel members discussed the types of fraud they are currently seeing. The number one consumer protection fraud is business imposter fraud – someone pretending to be a representative from a private company trying to get a customer's information. Romance fraud, money mules, and ID theft continue to increase along with fraud related to cryptocurrency, business email compromise, elder fraud, and use of false documentation. Partnerships are key to trying to detect and deter these fraud schemes.



The final panel discussed the financial flows tied to fentanyl and other illicit drugs. Generally, the panel noted indicators to be on the lookout for which include transactions, such as purchases of chemicals; wires to China; using bank wires; payments through MSBs; online payment services; and use of cryptocurrency. Red flags include cash payments, unusual payments to cryptocurrency exchanges or wallets, and unusual online transactions. For law enforcement, their relationships with financial institutions as well as with foreign law enforcement are so important in order to get insights into accounts.

Human Trafficking and Modern Slavery

Bob Pasley

On October 19th the U.S. Capital Chapter held a luncheon hosted by Allen & Overy partner, Jonathan Lopez, with guest speaker Matt Friedman, CEO of The Mekong Club, who provided a presentation on human trafficking and modern slavery.

Mr. Friedman, who has had over 30-years of experience in combatting and providing instruction in the area of human trafficking and modern slavery, provided some important statistics. For instance, he noted that there are over 40 million people in slavery today who are subject to physical and sexual violence. They are forced to work, for example, on fishing boats, as agriculture workers, as domestic workers, and in brothels as sex workers under threat of physical harm to themselves or their families. Their movements are restricted, their identity documents (such as passports) are taken from them, and their wages are withheld from them. Approximately 25% of modern slaves are children and approximately 25% of modern slaves are forced to work in the sex trade.

Asia contains approximately 62% of people held worldwide in modern slavery and the U.S. has approximately 403,000 people in bondage or slavery. The rate of worldwide exploitation is an astounding one person every four seconds, or 9.2 million each year.



There is approximately \$150 billion in profits to be made each year from slavery, but only \$350,000 in funding to combat it – representing only 0.23% of the estimated profits.

Awareness of the problem is growing and there are stronger laws being passed – such as in Canada and the EU, with large fines and penalties being assessed, including against banks. For instance, a bank in Australia was recently fined the equivalent of \$1.3 billion for its involvement in facilitating human trafficking and top bank officials were forced to resign. Training in companies is increasing in complexity, with the focus now shifting to have them look further down their supply chain with regard to the sourcing and manufacturing of their products and third party services used such as transportation of goods and cleaning staff in hotels and other premises.

In addition, class action lawsuits are growing, as well as legal action against hotels where human trafficking is found to be occurring. NGOs are also helping considerably. But the private sector needs to be more involved.



Mr. Friedman encouraged the audience to be vigilant and aware of the warning signs of human trafficking. One example is of a man who checked into a motel and saw a man dragging a 14-year-old girl into a nearby room. He reported it to the motel's front desk and, a little while later, police arrived, arrested the man and took the girl into protective custody. The man who reported the incident felt that he had never done anything so important as saving this young girl. When asked what he did for a living, though, the man said that he was a banker. When pressed, he said that he was in the fraud section of a bank and filed numerous SARs related to human trafficking. It was explained to him that filing SARs was extremely important and assisted in combatting human trafficking. So, unbeknownst to him, the man had been helping to combat modern slavery and human trafficking all along.

Mr. Friedman noted that the best thing the audience could do is to learn about the problem, tell other people about it, increase our awareness, be a responsible consumer, become a volunteer, and donate money to NGOs that are trying to counter human slavery.

Year In Review and Predictions for 2023

Barbara I. Keller, CAMS and Rachele Byrne, CAMS

On December 8, 2022, the US Capital Chapter held its annual Year-in-Review and predictions for next year in-person for the first time since 2019.

The Chapter was thrilled to have Dr. Louise Shelley kick off the afternoon as the keynote speaker. Dr. Shelly was in between sessions at the International Anti-Corruption Conference (IACC) and so it was very apropos for her to talk about corruption and developments in 2022. Although many countries imposed unprecedented sanctions this year after the Russian invasion of Ukraine, corruption goes so much deeper than oligarchs and yachts. The role of facilitators/enablers is so important and must be addressed. This is why the ENABLERS Act in the US Congress must be passed. There were also numerous notable corruption indictments in 2022. There has been more state involvement in illicit trade of essential items, such as counterfeit masks. This damages the legitimate economy. Beneficial ownership rules were also a newsworthy development in 2022 but FinCEN still has a lot more work to do. Dr. Shelley commented that environmental issues have been a big concern at the IACC. The funds that are being transferred to the developing world – will these be another mechanism for stealing and money laundering? We need to remain vigilant to make sure this doesn't happen.

The regulatory roundtable was moderated by Chapter Board member Lauren Kohr, with representatives from the Federal Reserve, FDIC, and OCC. We learned that new updates to the FFIEC manual are coming in the new year. Cyberthreats are a continuing risk and ransomware has seen an increase in 2022. Panelists encouraged attendees to use two-factor authentication to protect themselves. With regard to cryptocurrency, it's not about the transactions themselves but, rather, who's doing them. These are transactions outside of the regulatory perimeter but eventually they have to interact with the



traditional banking sector. There is pressure on banks to cut compliance costs and take on new business – to say it’s a complex risk environment is the understatement of the day. All regulatory agencies are concerned about the relationship between Fintech companies and banks. Data quality absolutely matters – banks are encouraged to try to map data flows to ensure there’s integrity in the data and to ensure they’re meeting regulatory requirements. Suspicious activity monitoring cannot be monitored without evaluating data quality. Final thoughts panel members mentioned as we look to 2023 include a heads up that new rulemakings and major changes in the AML regime are forthcoming because of the AML Act and banks should talk to their exam team early and often. Banks are also advised to look internally at their own risk profile.

The financial roundtable was moderated by Chapter Board member Les Joseph with panel members from the Fintech and consulting communities. We should expect lots of rulemakings coming down the pike - FinCEN should issue the notice of proposed rulemaking (NPRM) for access to the beneficial ownership registry any minute. After that FinCEN will have to issue revisions to the CDD rule to adjust for the registry. FinCEN released the national priorities in June 2021 but has yet to issue the proposed rule. We should expect changes to the Program rule in the new year. There was pushback on the ENABLERS Act, so it wasn’t included in the National Defense Authorization Act, as had been hoped. There is risk arbitrage in the crypto space – they are going to less regulated areas. One panelist commented that, in his view, the SEC is the best agency to be the crypto regulator in an umbrella sense.



The law enforcement roundtable was moderated by Chapter Board Co-Chair Dennis Lormel with panel members from various federal law enforcement agencies, including IRS-CI, HSI, and FBI. The panelists spoke about the priorities for their agencies in 2023, including conducting more interagency trainings and ensuring more law enforcement agents are CAMS certified. Financial crime topics expected to continue to dominate the investigative focus of law enforcement in 2023 were cybercrime, organized retail crime, fraud (i.e., elder fraud, healthcare fraud, and romance scams), and complex corporate crime. All the panelists agreed that fusion efforts, like the joint interagency cybercrime initiative and new advanced collaboration data center, continue to be key tools to aid law enforcement in combatting financial crime. The panelists also discussed the ongoing issue with staffing at agencies and the importance of recruiting new talent to join the public sector.



The last panel was a fireside chat between John Byrne, Chairman of the AML RightSource Advisory Board, and the Director of National Security Policy from the U.S. House Financial Services Committee. Legislative priorities in 2022 were focused on oversight of the implementation of the AML Act of 2020, including creation of the Beneficial Ownership database and access to it, as well as working to pass the provisions in the SAFE Banking and ENABLERS Acts. On the latter two, the panelist stated that, while time was running out to pass the legislation this year, they remain priorities for the current House Financial Services Committee. However, given the change in majority party expected to take place in January 2023, further progress on the passage of the legislation remains in doubt. Other topics discussed included trade-based money laundering, de-risking, real estate, and potential cryptocurrency regulation.



*Thank
You*

Allen & Overy, AML RightSource, John Byrne, John Davidson, FinCEN, FBI-Counterterrorism Division, FDIC, Federal Reserve, Matt Friedman, Jonathan Helmstetter, IRS-CI, HSI-Transnational Organized Crime Division, Les Joseph, Kaufman-Rossin, Barbara Keller, Lauren Kohr, Danielle Camner Lindholm, Dennis Lormel, Debra LaPrevotte, Jonathan Lopez, OCC, Torchlight AI, Sepideh Rowland, Sarah Runge, Dr. Louise Shelley, Dan Stipano, and Johnathan Willis