EIGHTH LAW ENFORCEMENT EDITION

ACAMS® TODAY

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

JUNE–AUGUST 2018
VOL. 17 NO. 3

A publication of the Association of Certified Anti-Money Laundering Specialists® (ACAMS®), Miami, FL, USA

www.ACAMS.org
www.ACAMSToday.org

ACAMS | Risk Assessment®

acamsriskassessment.com

MEASURE, UNDERSTAND & EXPLAIN YOUR MONEY LAUNDERING RISKS

This first-of-its-kind solution helps your institution:

- Identify risks within and across all lines of business
- Mitigate risk by filling in the gaps in your detection and prevention controls
- Present trusted reports that are up-to-par with the latest global regulation and guidance
- Clearly communicate risk to all stakeholders through standardized and automated presentation-ready reports

Schedule a product demo:
riskassessment@acams.org

No one can help you Know Your Customer like Thomson Reuters

With a total solution from a single provider, nothing slips through. No gaps, no communication break-downs, no lapses in coverage. There is nowhere for bad behavior – or bad players – to hide.

No one delivers trusted, effective, end-to-end KYC solutions like Thomson Reuters.

tr.com/kyc

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®

JUNE–AUGUST 2018 VOL. 17 NO. 3

ACAMS TODAY

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

The award-winning *ACAMS Today* magazine is designed to provide accurate and authoritative information concerning international money laundering controls and related subjects. In publishing this work, neither the authors nor the association are engaged in rendering legal or other professional services. The services of a competent professional should be sought if such assistance is required. *ACAMS Today* is published four times a year for ACAMS members.

To join, contact: ACAMS
Brickell City Tower
80 Southwest 8th Street
Suite 2300
Miami, FL 33130

Tel. 1-305-373-0020
Fax 1-305-373-7788
Email: info@acams.org
Websites: www.ACAMS.org
www.ACAMSToday.org
Twitter: @acamstoday

To advertise, contact:
Andrea Winter
Tel. 1-305-373-0020 ext. 3030
Email: awinter@acams.org

ACAMS®

UNLOCK THE FUTURE OF AML

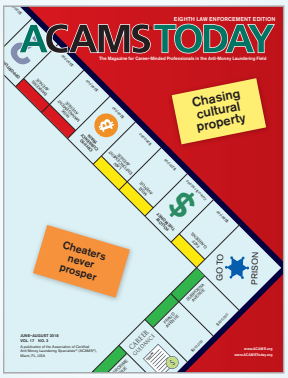
Protiviti are proud to be sponsoring ACAMS 14th Annual AML & Financial Conference in Europe

protiviti®

Face the Future with Confidence

CONTENTS

ON THE COVER:



Chasing cultural property

Cultural property is one more commodity that can be leveraged in financial crime.

Page 26

Cover design: Wendy Meyer

Erik Barnett: The importance of public-private partnerships
Regional Head of Europe for Financial Crime Threat Mitigation of HSBC, Erik Barnett, talks about money laundering risks in Europe, counterterrorism and virtual currencies. Page 14

Cryptocurrencies and the BSA
What compliance professionals need to know about cryptocurrencies when filing suspicious activity reports. Page 16

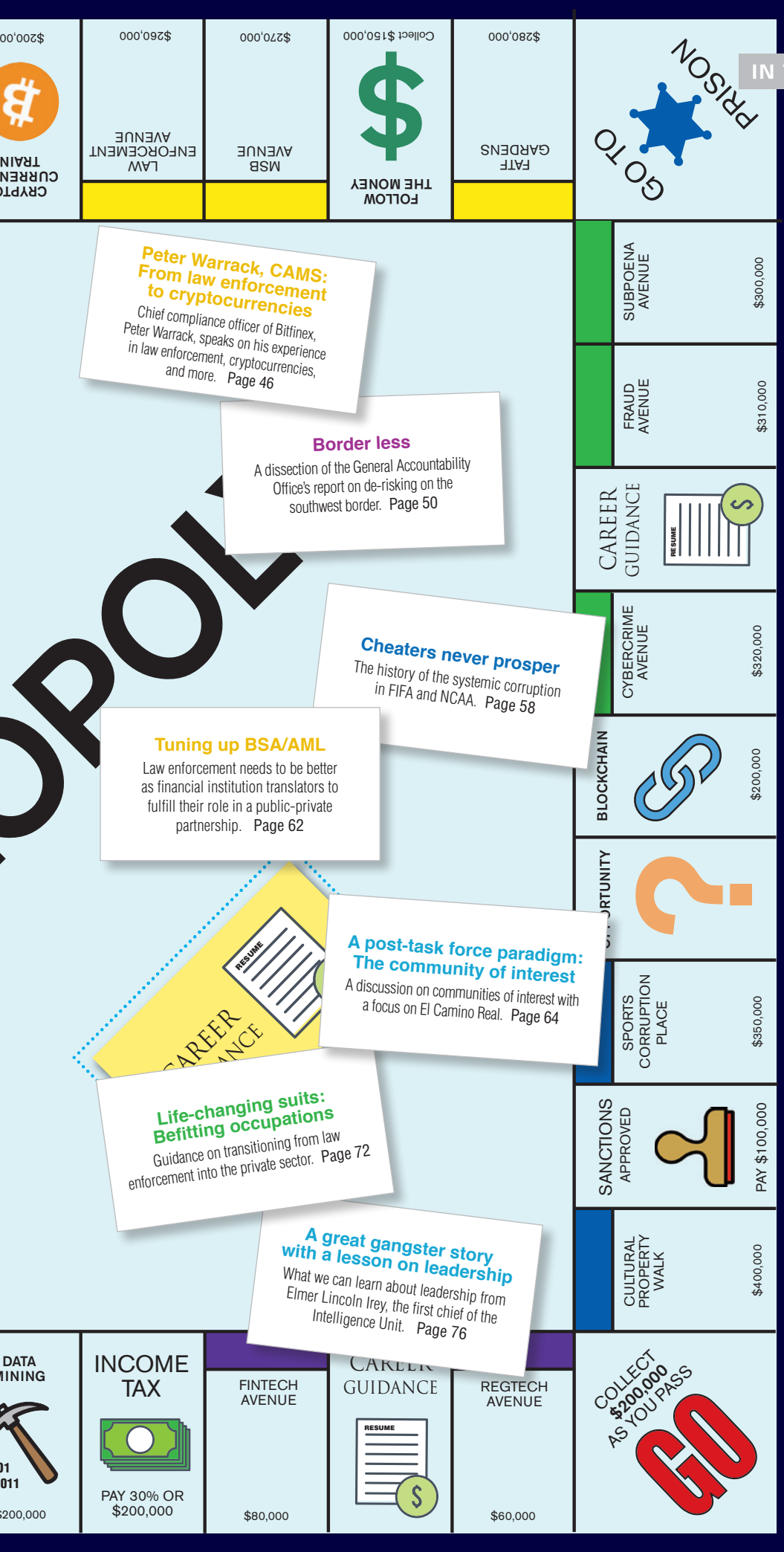
Organ trafficking: The unseen form of human trafficking
How organ trafficking occurs and what is being done to address this lesser discussed form of human trafficking. Page 22

Real considerations for law enforcement in seizing virtual currency
A background on virtual currency for law enforcement and how to use this knowledge when seizing virtual currency. Page 30

Challenges and best practices surrounding the BSA/AML independent reviews
What are the expectations around transaction testing and learn how you can ensure an appropriate independent review scope. Page 34

Are you missing the smoking gun?
Understanding the need to evolve the current subpoena language, how to improve the quality and accuracy of information obtained and used in a financial-related investigation. Page 36

Cybersecurity: Confronting impersonation fraud as banks reorganize
How organizational changes in banks could open the door to cyber fraud and tips on how to prevent this. Page 40



IN THIS ISSUE

ASPECTS OF ASIA

EUROPE

KNOW YOUR CHAPTER

Contents design: Victoria Racine

Each article is associated with a square on the AMLopoly game board. Can you guess which square pertains to the article you are reading? Find the answer at the end of the article.

Let the games begin

This year has and continues to be an important one for competition. Earlier this year, the world watched the Winter Olympics in South Korea. June marks the beginning of the World Cup in Russia. Though I have never competed at the level of these elite athletes, I have always been competitive. Growing up I played a number of sports and thrived under the feeling of competition. After my competitive years in sports fell by the wayside, I carried my competitive spirit to game night with friends, where we gather and play board games—of course this is just for fun, but finishing as the victor, even if it is a board game, is quite satisfying. Competition can encourage the betterment of oneself like in schooling or in an industry. It can urge the development of new skills or sharpen existing abilities.

Every year *ACAMS Today* (AT) publishes a special Law Enforcement (LE) edition. I am proud to say this will be our eighth issue. We wanted to inspire a little friendly competition among financial crime prevention professionals in their role to thwart criminals who commit financial crimes, and as such, I am proud to showcase—AMLopoly. This imaginative board features and displays the informative articles found in this insightful edition. The cover article, *Chasing cultural property,* highlights the valiant efforts of the agents of Homeland Security Investigations (HSI) tasked with recovering trafficked antiquities and the anti-money laundering (AML) implications that are often overlooked in the public discourse of these crimes.

The second cover article, *Cheaters never prosper,* revisits the topic of corruption in professional sports. There have been a number of new allegations of corruption in the U.S. collegiate levels of basketball. The article analyzes the systemic failures in various sports corruption scandals and the implications for the financial sector.

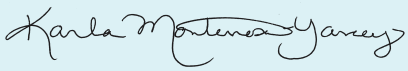
This eighth LE edition also contains a somber topic that needs to be discussed. The article, *Organ trafficking: The unseen form of human trafficking,* highlights the atrocities individuals endure at the hands of transnational organized crime groups. The authors share why this is a lucrative business, money laundering indicators and how organ trafficking fits into the broader definition of human trafficking.

Cryptocurrency, one of the most talked about topics this year, is in full display in the AT LE edition. We have three articles about the topic: *Regulating a game changer—Europe's approach to cryptocurrencies, Cryptocurrencies and the BSA* and *Real considerations for law enforcement in seizing virtual currency.* Each one of these articles presents a different angle about the topic of cryptocurrency. In addition, we have the article, *Cybersecurity: Confronting impersonation fraud as banks reorganize,* which walks you through how to target scam alerts, banks' vulnerabilities to impersonation fraud and key takeaways on what to consider to protect your institution from cyberattacks.

An AT LE issue would not be complete without interviews from subject-matter experts who also have a background in LE. I had the opportunity to interview Erik Barnett, regional head of Europe for Financial Crime Threat Mitigation (FCTM) at HSBC, about money laundering risks in Europe, counterterrorism and the importance of public and private partnerships. I also interviewed Peter Warrack, chief compliance officer of Bitfinex, on his experiences in LE, banking and cryptocurrencies.

Finally, I wanted to highlight the career guidance article titled: *Life-changing suits: Befitting occupations,* which describes to professionals who have worked in the public sector for years how to transition into the private sector and how to best use the skills they have learned while working in the public sector to continue their efforts in the fight against financial crime.

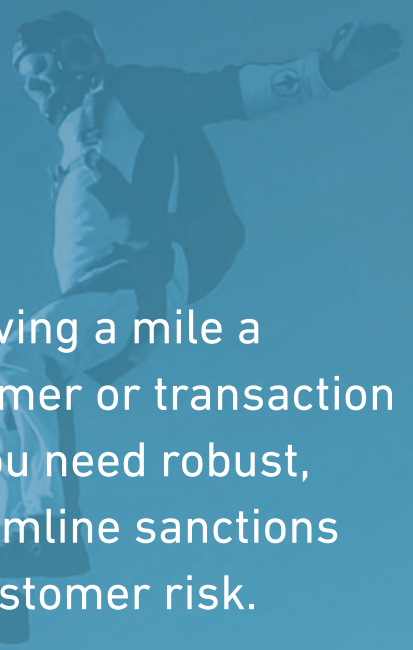
The AT LE issue is always one of my favorite editions of the year, whether we work in the private or public sector, whether we work for banks or a money services business, we are all competing to vanquish the financial criminals. May we continue to be the best competitors in thwarting financial crime.



Karla Monterrosa-Yancey, CAMS
editor-in-chief
Follow us on Twitter: @acamstoday

P.S. Do not forget to vote for the *2018 ACAMS Today Article of the Year Award.* Cast your vote by visiting: www.acamsconferences.org/vegas/awards/

CSI KNOWS BUSINESS IS RISKY.



CSI

Your business may be moving a mile a minute, but one bad customer or transaction can stop you on a dime. You need robust, integrated tools that streamline sanctions screening and mitigate customer risk.

CSI's WatchDOG® Elite gives you the platform you need to make KYC and identity verification less daunting—and business less risky.

www.csiweb.com/riskybusiness

Stuart G. Berman, CAMS, CFE
Chicago, IL, USA

Stuart Berman began his career as a securities enforcement auditor with the Illinois Securities Department. As an auditor, he specialized in detecting promissory note Ponzi schemes and worked on several multi-million dollar schemes.

Berman used this experience toward what would be a long and successful career as a special agent with the U.S. General Services Administration (GSA) Office of Inspector General (OIG) in Chicago. In that role, he planned, organized and conducted complex white-collar investigations concerning GSA contracts, personnel, contractors and contractor employees. These investigations involved a wide variety of fraud allegations, including bribery, kickbacks, inferior quality-product substitution, cost mischarging, anti-trust violations, credit card fraud, diversion of excess government property and money laundering.

Berman became the special agent in charge for the GSA OIG in August 2008. He supervised the GSA OIG regional criminal, civil and administrative investigative program, encompassing six Midwestern states and 12 judicial districts. He was responsible for managing investigative business operations and program functions as well as administrative operations, including budget and personnel decisions. Berman provided technical advice, counsel and support to secondary management teams and to the criminal investigative and administrative support units. After a highly successful and award-winning law enforcement career, Berman retired from the GSA OIG at the end of April 2018.

In May 2018, Berman joined BKD CPAs & Advisors, a national accounting and advisory firm with 36 offices nationwide, as a director in the Forensic & Valuation Services practice. He also serves as the practice lead for the Chicago office.

Berman is a summa cum laude graduate of DePaul University with a bachelor's degree in liberal arts and sciences.

Elisa Castrolugo
Houston, TX, USA

Elisa Castrolugo, a former federal criminal prosecutor and immigration judge, is an international legal consultant in the areas of anti-money laundering (AML), counter-terrorist financing (CTF), anti-bribery, anti-corruption, compliance, international cooperation and EU data privacy law.

Castrolugo joined the U.S. Department of Justice (DOJ) in 2005 as an assistant U.S. attorney (AUSA) and was the first AUSA to be selected through the DOJ Honors Program. In her decade-long career as AUSA, she successfully prosecuted felony criminal cases, including international money laundering, trademark infringement and fraud offenses (e.g., wire, mail, bank, tax refund, identity theft).

She completed three special assignments with the DOJ's Criminal Division, receiving the *Attorney General's Distinguished Service Award* for her work on electronic surveillance issues. She briefly served as the acting judicial attaché in Mexico and then spent one year in Colombia and Paraguay as the South America legal advisor on CTF and AML.

Castrolugo is a graduate of Columbia Law School and the University of Texas at Austin. She is a veteran of the U.S. Air Force and the Texas Air National Guard. She is fluent in Spanish and conversant in Portuguese.

Andrew McDonald
London, U.K.

Andrew McDonald served over 30 years with the Metropolitan Police Service, of which 20 years were with specialist covert and overt operations within counter-terrorist or organized crime teams at New Scotland Yard. He retired in January 2017 as head of specialist investigations of the U.K. National Terrorist Financial Investigation Unit (NTFIU) at SO15 Counter Terrorism Command, New Scotland Yard. In this role, he had strategic and tactical oversight of all financial investigation and crime disruption investigations to identify, arrest and charge or disrupt terrorist offenders and their criminal associates.

In a previous role as head of the London Metropolitan Police Fraud Squad, McDonald was responsible for designing their current operating model for fraud and cybercrime and assisted in its implementation.

Following his police retirement in January 2017, McDonald was appointed as the compliance officer for the U.K. Independent Parliamentary Standards Authority—a statutory role that he undertook on a part-time basis until May 2018.

Over a number of years, McDonald has designed and delivered bespoke training and advisory services to employees of all levels in many public sector and commercial organizations in the U.K. and overseas. He has enjoyed co-authoring, contributing to, and delivering webinars on five ACAMS certificate courses.

McDonald holds Bachelor of Science and Master of Business Administration degrees and is a fellow of the Chartered Institute of Management.

Kent Stern, CAMS-FCI
Boca Raton, FL, USA

Kent Stern is the director and lead data-mining architect for CodeCenters International. In 1987, he started the company with a small team of engineers who specialized in designing software for aircraft, ship and container routing. Today, most of his time is spent auditing machine learning and data security platforms related to anti-money laundering (AML) software and evaluating legal proceedings that are inevitably produced after a data breach has occurred.

Based primarily in the U.K., he travels between offices in the U.S., the Middle East and India. His work has taken him to every corner of the globe and into every conceivable area of data analysis, but the ability for him and his employees to keep up with the latest technology has always been a major part of his corporate philosophy. This past year, he completed the ACAMS Advanced Financial Crimes Investigations Certification (CAMS-FCI) and finished a four-country tour lecturing on building a sound defense when dealing with litigation related to digital AML processes. He is a (ISC)² Certified Information Systems Security Professional (CISSP) and has been an active Microsoft Certified Trainer since 1999. He is also an advisory board member for the Cybersecurity for Business Program at the Muma College of Business at the University of South Florida.

DID YOU KNOW WE ARE NOW ACCEPTING NOMINATIONS FOR THE ACAMS TODAY ARTICLE OF THE YEAR AWARD?

QUIZ

Test your AML/CTF knowledge today!

Visit ACAMSToday.org to take the latest quiz

1. **Which of the following is a human trafficking red flag shared by FINTRAC?**
   - A) Frequent payments in multiples of small amounts to online advertising and promotional services
   - B) Payments for short accommodation stays and/or stays in multiple cities in a relatively short time
   - C) Frequent purchase for airline, train and/or bus tickets, possibly for multiple individuals, in relatively short timelines
   - D) All of the above

2. **Which of the following are key issues to ensure the effectiveness of a compliance testing program?**
   - A) Tone at the top
   - B) Get the best out of technology
   - C) Work effectively with other control functions
   - D) All of the above

3. **The flow of gold imports into the U.S. stems primarily from Europe and Asia; however, recent reports have noted an increase of illegal gold from _____.**
   - A) Central America
   - B) South America
   - C) Africa
   - D) Australia

QUIZ

Fighting financial crime requires honoring those who protect and serve

The *ACAMS Today* (AT) Law Enforcement (LE) issue offers an annual opportunity to pause and take note of ACAMS' longstanding partnership with the LE community, and to express our appreciation for the men and women in the public sector dedicated to fighting crime, particularly financial crime.

While there has always been a connection between LE and financial institutions, that relationship became a true partnership after September 11, 2001, when compliance officers at U.S. financial institutions were virtually deputized under the USA PATRIOT Act.

Subsequently, new leadership on anti-money laundering (AML) and counter-terrorist financing (CTF) emerged from the parliaments of the EU and U.K. in the wake of brutal terror attacks in France, Belgium, Germany and the U.K. These initiatives also envision greater private sector cooperation with LE; for example, those realized in the U.K.'s Joint Money Laundering Intelligence Taskforce (JMLIT) and the EU's Europol Financial Intelligence Public Private Partnership.

ACAMS is proud to have a role in this flourishing collaboration. In addition to offering specialized training for anti-financial crime (AFC) professionals from the private and public sectors, ACAMS brings both sectors together at our conferences, chapter meetings and other events, all designed to serve as trusted platforms for the exchange of information and expertise.

This AT LE issue suggests the breadth of the material our community is required to master, including a fascinating account of the U.S. Department of Homeland Security's role in repatriating to Iraq stolen Mesopotamian artifacts. At conferences, our sanctions sessions focus on enabling professionals to make the connections that will flag unacceptable transactions. For both public and private sector practitioners, that expertise is supported as much by a grasp of intricate regulations and familiarity with trade finance as by an understanding of the social, political and historical landscape in which these transactions are taking place.

Reflecting the critical and demanding nature of this work, and their accountability, AFC professionals at financial institutions have seen a significant rise in resources and respect over the past 17 years. For the public-private partnership to achieve its full potential, however, the important contributions of our colleagues in the public sector must be held in similar high regard, and accorded the same respect.

Now more than ever, the increasing sophistication of financial criminals requires that LE have the capacity to recruit the best and the brightest. To be sure, young people considering a career in LE must be drawn to a higher calling. But in addition to a commitment to "serve and protect," they must also have the capacity and curiosity to engage with vast amounts of emerging information across disciplines, from the social sciences and the arts, to mathematics and technology.

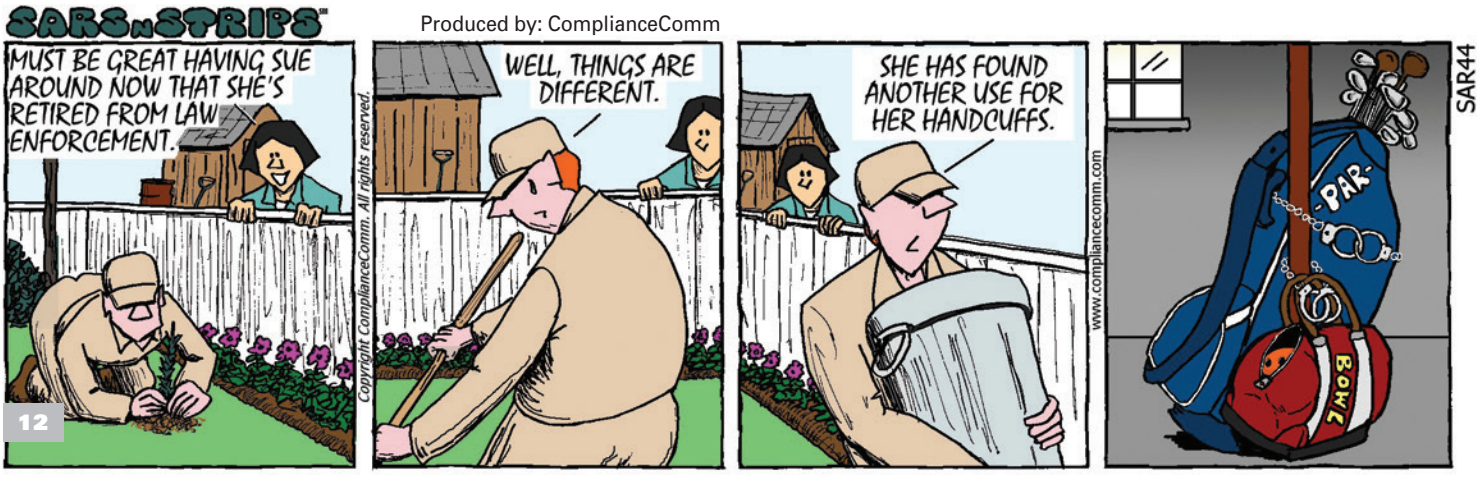
ACAMS will continue to provide platforms for the exchange of information, expertise and best practices to ensure the integrity of our financial systems. The recent Hollywood, Florida conference tackled artificial intelligence and machine learning, human trafficking and marijuana. As I write, I am preparing for a panel with AFC heads at major global banks for the *ACAMS 14th Annual AML & Financial Crime Conference Europe* that will cover complex emerging financial crime threats and the adoption of technology, many of which could not have been imagined 20 or even 10 years ago.

AFC compliance officers must face these challenges—and those yet to emerge—in partnership with capable, sophisticated LE officials.

Helping us face those challenges over the decades have been speakers from the U.S. Department of Justice, the Federal Bureau of Investigation, Homeland Security, the U.K.'s National Crime Agency, Metropolitan Police, Europol, the Washington/Baltimore High Intensity Drug Trafficking Area (HIDTA), Northern Virginia's Financial Initiative (NVFI), and the IRS's Criminal Investigations division. Forgive me if I have omitted anyone, which I almost certainly have given the level of global LE participation over the years.

On behalf of the AML community, we are privileged to acknowledge all the fine public servants whose dedication and professionalism help make our world a safer place to live and work.

Kieran Beer, CAMS
director of editorial content
kbeer@acams.org
Follow me on Twitter: @KieranBeer



Managing pot is not business as usual

The marijuana industry is at a crossroads. Until federal and state legislation come together or further guidance is available, uncertainty remains. **And risk.**

Know your risk with SBS' new marijuana related business (MRB) list offering. With the inclusion of Dow Jones and MRB Monitor list options, SBS' list management product provides valuable insight for identifying and managing this expanding population of high-risk customers. And it's just another example of SBS' robust technology at work.

Find out how SBS' anti-money laundering and compliance solutions can help you identify, assess and manage risk.

Contact **sales@safe-banking.com** or visit **www.safe-banking.com** to learn more.

SBS®
SAFE BANKING SYSTEMS

Thinking Ahead of the Risks

ERIK BARNETT: The importance of public-private partnerships

ACAMS Today spoke with Erik Barnett, regional head of Europe for Financial Crime Threat Mitigation (FCTM) at HSBC, on money laundering risks in Europe, counterterrorism and virtual currencies. In this role, he leads professionals investigating financial crime, preventing fraud, and developing intelligence and analytics capabilities to proactively identify risk in 21 countries in HSBC's Europe region. FCTM is responsible for investigation, analytics and intelligence, as well as many of the systems engaged in fighting financial crime.

Prior to this role, Barnett was the attaché to the EU for the U.S. Department of Homeland Security and engaged extensively with European law enforcement and Europol on anti-money laundering (AML) and counterterrorism as well as emerging risks.

Formerly, Barnett was the assistant deputy director of U.S. Immigration and Customs Enforcement, where his portfolio included the criminal investigative function of Homeland Security Investigations, a federal law enforcement agency combating illicit trade, travel and finance.

For fifteen years, Barnett was a criminal prosecutor, working ultimately at the U.S. Department of Justice where he led units investigating narcotics trafficking and transnational violent crime. Barnett also worked for over five years in the U.S. Congress and was an adjunct faculty member at two law schools, teaching legal writing and trial advocacy.

ACAMS Today: ***Part of your responsibilities at HSBC include identifying risks in the European region. At this time, what are the biggest money laundering risks facing the area?***

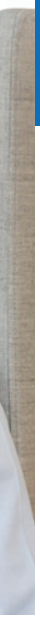
Erik Barnett: The risks are many and varied and include transnational, regional and global threats. Transnational crime groups and other bad actors are drawn to global banks such as HSBC due to our size, product offerings and their need to legitimize criminal finances. In terms of criminal monetary loss or gain, fraud, tax evasion, market abuse and trade-based money laundering are still the largest crime areas across the region, but also significant is the distribution of illegal drugs, terrorist finance, human trafficking and smuggling, as well as the commission of large-scale fraud and movement of those proceeds. It remains a complicated landscape.

AT: ***How is your institution mitigating those risks and has law enforcement played a role in assisting to mitigate those risks?***

EB: At HSBC, we have a fundamental responsibility to help protect the integrity of the financial system on which we all depend. We're using our knowledge and global reach to lead the fight against financial crime, which will benefit the bank, our customers and society at large. Consistent with privacy laws, we have the ability to look across borders and within our accounts and transactions for crime typologies that we've developed, often in consultation with law enforcement. HSBC believes that we can tackle financial crime most effectively if we do it collaboratively. We are strong believers in public-private partnerships and the wider information sharing initiatives. We need to help one another to align our understanding and reporting to assist law enforcement, including sharing of intelligence and understanding to help us use our data better and to report back clearer suspicion.

AT: ***Are there legislative issues on the horizon you believe will impact the banking industry's fight against financial crime?***

EB: The information exchange mechanisms within the U.K. Joint Money Laundering Intelligence Taskforce (JMLIT), of which HSBC is a founding member, have brought concrete results in helping the public sector to respond to operational priorities such as human trafficking and serious security threats, including terror financing. They have also improved the private sector's financial crime risk-management programs. However, to build on this success in the U.K. and wider, countries should consider the provisions for information sharing in three key areas: between the private sector and governments, between banks and within banking groups. We have seen progress at the international level through the Financial Action Task Force (FATF). Nevertheless, more could still be done to ensure



> CLEARLY, THE MOST EFFECTIVE WAY FOR FINANCIAL INSTITUTIONS TO IDENTIFY POTENTIAL TERRORIST ACTIVITY IS THROUGH COLLABORATION WITH LAW ENFORCEMENT AND SECURITY SERVICES

that the benefits of public-private partnerships are truly delivered. We already have good language in the Fourth AML Directive in the EU, on information sharing among government and financial institutions. We would like to see that thoroughly implemented, and executed.

AT: ***Recent terrorist attacks in Europe and elsewhere have involved lone, rogue actors (or only two or three perpetrators) utilizing a small amount of funds and resources to conduct attacks. What kind of due diligence can financial institutions implement to catch or prevent these kinds of funds from flowing through their institutions?***

EB: Clearly, the most effective way for financial institutions to identify potential terrorist activity is through collaboration with law enforcement and security services. Increased intelligence sharing and using structures such as the JMLIT in the U.K. can act as a force multiplier in proactively identifying individuals planning an attack. In the aftermath of an attack, it can also point to a wider network that may have been involved and prevent a "second wave" event. This increased intelligence sharing must be predicated on mutual trust and understanding of respective legal and regulatory obligations. The emergence of public-private partnerships is definitely helping to shape this.

AT: ***What measures have financial institutions and law enforcement taken to work together in thwarting future terrorist attacks?***

EB: HSBC was a founding member of both the JMLIT and Europol's Financial Intelligence Public Private Partnership and we advocate for these mechanisms in other parts of the world. The real power we have against financial crime and transnational criminals is the collective ability to assist one another in a proportionate and lawful manner to ensure we protect the integrity of the financial system and better serve our customers and communities.

AT: ***You have had an extensive career in criminal investigations, what is the most exciting or interesting case you have worked on?***

EB: Because the criminal cases have been so varied and had so many fascinating angles, it's not possible or fair to select one as the most exciting or interesting. The most important thing—what made it such an amazing career—was working through the challenges of the law and the facts, as a team of prosecutors and police, to achieve the right result. In addition, that's fortunately what I've also found at HSBC, where the approach and overall objective is very similar.

AT: ***Let us talk about virtual currencies (VCs) and your thoughts on their global emergence.***

EB: HSBC is monitoring the development of virtual and digital currencies such as bitcoin as well as regulations governing their use. With the global emergence of VCs, it is recognized that mainstream companies, such as Amazon, Expedia, Microsoft and local "mom and pop" shops are beginning to accept VC as a form of payment. Investors will seek high returns with VCs. In countries where use of VCs is permitted by the authorities, we expect any customer transacting in them to comply with all applicable laws and regulations, just as they would for transactions denominated in traditional legal tender.

AT: ***At this given time in AML history, what is the most important thing an institution can do to combat money laundering and terrorist financing?***

EB: The only way for financial institutions to effectively combat money laundering and terrorist financing, as well as a range of other economic crimes, is through working collaboratively with partners in law enforcement and industry. The positive impact of public-private partnerships in providing a forum for the timely sharing of financial crime intelligence has been highlighted by recent FATF papers as well as nongovernmental organizations. Initiatives established in the U.K., U.S., Hong Kong, Australia, Canada and Singapore have already produced significant results in terms of disruption of criminal organizations and seizure of criminal funds. The next step is exploring mechanisms that allow the transnational sharing of financial and law enforcement intelligence through a centralized body, making it even more difficult for criminal networks to operate across borders.

Further, financial institutions must be encouraged to be more creative and agile when it comes to effectively analyzing the vast amounts of data held within various systems. By being more proactive and data analytics-led, HSBC and other financial institutions will be better able to identify customers and transactions of concern.

AT: ***What do you like to do when you are not saving the world from financial criminals?***

EB: The challenge in combating financial crime is so geopolitical, many events have an impact across various levels (the bank, national security, society). So even on a weekend I might have to consider the potential risk created by an incident, whether it's a terrorist attack or a political election/scandal. But, spending time with family and enjoying my hobbies—reading, exercising and just walking the dog—that's what you would find me doing and they are definitely key to ensuring a healthy work-life balance.

Interviewed by: Karla Monterrosa-Yancey, CAMS, editor-in-chief, ACAMS, Miami, FL, USA, kmonterrosa@acams.org

Cryptocurrencies and the BSA

In late 2008, a person (or persons), writing under the nom de guerre Satoshi Nakamoto, published a nine-page technical paper purporting to have solved the double-spending problem of electronic funds transfers, which, hitherto, necessitated the intervention of financial institutions to allow for online payments. With this solution, Nakamoto claimed that, "online payments [can] be sent directly from one party to another without going through a financial institution."[1] He called his idea Bitcoin.

Nakamoto was not the first to come up with the idea of a method for cryptographic funds transfer; indeed, ideas for such payment methods go back to at least the early 1980s.[2] However, the timing of Nakamoto's paper—just as the 2008 financial crisis was going full steam—was serendipitous. Faith in the financial system had ebbed severely, and the idea of a payment method and store of value not tied to the apparently failing system may have been just the solution needed. Furthermore, the distributed ledger, dubbed blockchain, was Nakamoto's novel method of solving the double-spending problem; it necessitated a high, and increasing, level of computer-processing capabilities as well as widespread internet use to be viable.

Since the publication of Nakamoto's paper, there has been an explosion in cryptocurrencies, with over 1,500[3] currencies available, and more seeming to come by the day. In addition to online exchanges, cryptocurrencies can be purchased through ATMs, bitcoin futures can be traded on the Chicago Mercantile Exchange (CME) or Chicago Board Options Exchange (CBOE), and swaps can be traded via LedgerX, assuming one has the 100 percent margin required to do so. This, in turn, has brought exposure to cryptocurrencies to a variety of financial institutions that have previously never dealt with such creatures and are not entirely sure how to tame them. More specifically for anti-money laundering (AML) professionals, it is not always clear how cryptocurrencies fall into Bank Secrecy Act (BSA) compliance and reporting requirements. The Financial Crimes Enforcement Network (FinCEN) has issued guidance in this area, but this has been directed to

[1] Satoshi Nakamoto "Bitcoin: A Peer-to Peer Electronic Cash System," Bitcoin, 2008, p. 1, https://bitcoin.org/bitcoin.pdf

[2] Victor Dostov and Pavel Shust, "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?" *Journal of Financial Crime*, Vol. 21, No. 3, 2014, p. 250.

[3] www.coinmarketcap.com, accessed February 8, 2018.

cryptocurrency exchanges,[4] miners,[5] payment processors[6] and trading platforms.[7] What about financial institutions that are not engaging in any of these activities, but have clients who are? What are the BSA reporting obligations for those entities? These answers will need to come from the regulators. The purpose of this article is to highlight some of these issues, and to suggest possible avenues of mitigation for BSA officers.

Digital cash

In order to understand how cryptocurrencies might fit into BSA reporting, one needs first to understand what they are. This is not an easy endeavor, as cryptocurrencies are often defined by their function. In some cases they may be a commodity,[8] in others, a security.[9] For our current purposes, we will take Nakamoto's own designation and refer to cryptocurrencies as cash.[10] Cash is traditionally understood as paper notes and coins backed by government fiat and used as mediums of exchange. However, if we abstract out, as Nakamoto has done, and understand cash as any anonymous medium of exchange, then we have a better understanding of where cryptocurrencies fit into the money laundering cycle in general, and specifically to BSA reporting.

The meaning of anonymity requires a bit of exploration here, as both paper notes and cryptocurrencies are typically thought of as anonymous, though the latter is not entirely so. In their paper, *Cryptocurrencies: an unconventional challenge to the AML/CTF regulators?,* Dostov and Shust provide an excellent explanatory analogy:

> "[W]e need to draw a line between real anonymity and popular understanding of anonymous interactions. The latter is also called 'unlikability.' For example, numbered (yet, anonymous) accounts are intrinsically linked to their owners, if at least one transaction performed using this anonymous account can be traced to a real person (for example, if the owner is a frequent cocaine buyer but had a gross mistake of paying for the air ticket or hotel room from this same account) one can associate this account (as well as payments that were and will be made through it) with its owner."[11]

For cryptocurrencies, replace "account" in the quote above with "private key." Figure 1 further illustrates this distinction.

Cryptocurrencies, like paper notes, are only anonymous so long as they remain outside the financial system. They may be even less anonymous than notes and coins due to the digital signature left in the ledger by the transaction. Adam Ludwin, from whose article Figure 1 was taken, explains:

> "Average users should be aware that [bitcoin] is certainly less anonymous than cash. Meanwhile, dedicated users willing to go to extraordinary lengths can find ways to acquire and use bitcoin anonymously, but the open nature of the transaction ledger and other unknowns leave open the possibility that identities and activities once considered perfectly secure may be revealed at some point down the road."[12]

Given this digital trace, it may be more accurate to compare cryptocurrencies to cashier's checks rather than paper notes.[13]

The BSA attempts to remove some of the anonymity of other forms of cash by way of record keeping requirements, such as monetary instrument logs, currency transaction reports (CTR) and Reports of International Transportation of Currency or Monetary Instruments (CMIR). One way to assuage the problem of cryptocurrencies' pseudo-anonymous nature would be to require similar reporting for electronic cash transactions over a specified amount. This is in

CRYPTOCURRENCIES, LIKE PAPER NOTES, ARE ONLY ANONYMOUS SO LONG AS THEY REMAIN OUTSIDE THE FINANCIAL SYSTEM

[4] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FinCEN, March 18, 2013, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering

[5] "Application of FinCEN's Regulations to Virtual Currency Mining Operations," FinCEN, January 30, 2014, https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf

[6] "Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System," Financial Crimes Enforcement Network, October 27, 2014, https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf

[7] "FIN-2014-R011," Financial Crimes Enforcement Network, October 27, 2014, https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf

[8] "In the Matter of Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan," U.S. Commodity Futures Trading Commission, September 17, 2015, http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf

[9] "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," Securities and Exchange Commission, July 25, 2017, https://www.sec.gov/litigation/investreport/34-81207.pdf

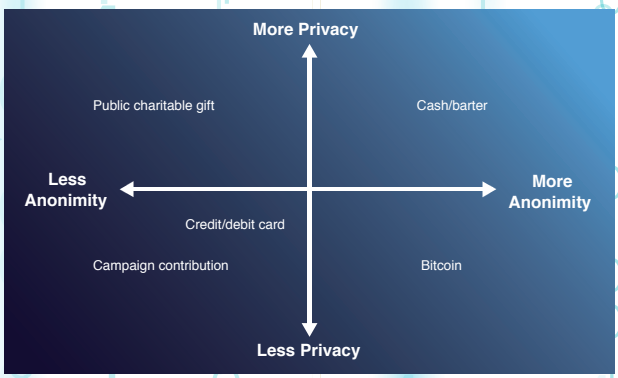
[10] The subtitle of Namakoto's paper makes this reference: "A Peer-to-Peer Electronic Cash System."

[11] Victor Dostov and Pavel Shust, "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?" Journal of Financial Crime, Vol. 21, No. 3, 2014, pp. 251-252.

[12] Ibid.

[13] Cashier's checks should also be understood as a form of cash given the anonymous nature of the instrument.

Figure 1

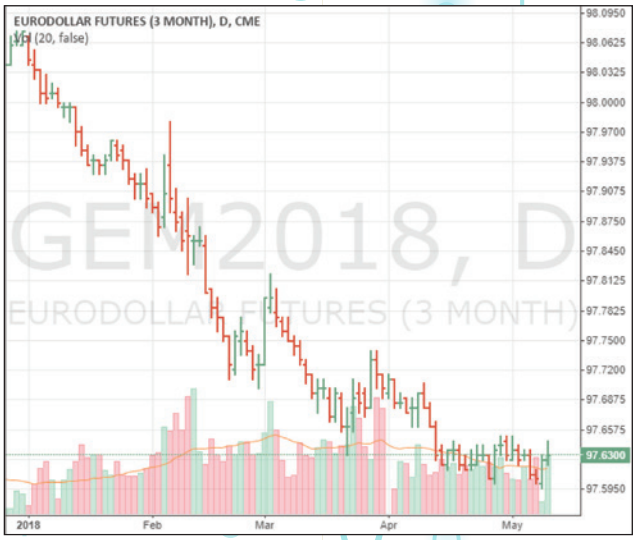


Source: Adam Ludwin, "How Anonymous is Bitcoin? A Backgrounder for Policymakers," *CoinDesk*, January 25, 2015, https://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/

Figure 2

Source: CME Group, http://www.cmegroup.com/trading/interest-rates/stir/eurodollar_quotes_globex.html [cmegroup.com]

Figure 3



Source: CME Group, http://www.cmegroup.com/trading/equity-index/us-index/bitcoin.html [cmegroup.com]

keeping with the recommendation put forth by the Financial Action Task Force (FATF) in their guidance on virtual currencies, suggesting that "AML/CFT controls should target convertible VC [virtual currency] nodes – i.e., points of intersection that provide gateways to the regulated financial system."[14]

Persons exchanging cryptocurrencies for fiat currency in the U.S. are already required to register as money services businesses (MSBs) with FinCEN, which subjects them to certain AML requirements. Expanding these requirements to include reporting of exchange transactions (e.g., cryptocurrencies to fiat, or between various cryptocurrencies) over a designated amount specified in a U.S. dollar equivalent would give law enforcement much greater insight into online cash movement, and bring requirements around cryptocurrencies more in line with those required of other types of cash.

Suspicious activity reporting

The heart of the BSA is filing suspicious activity reports (SARs) for regulators and law enforcement. Indeed, all the other requirements of the BSA (Customer Identification Program, know your customer, monitoring, training, etc.) act as the undergirding of SAR reporting. FinCEN has provided some guidance on SAR filings for cryptocurrencies, noting that "SARs filed by the various filing entities may provide valuable information related to accounts, ownership and other identifying information, and Bitcoin addresses associated with suspicious activity."[15] While this sheds light on the points of information FinCEN would like to see reported, it is not clear what, if anything, unique to a cryptocurrency transaction would trigger the need for an investigation and possible filing.

For starters, is the purchase or use of cryptocurrencies suspicious on its own? Governments around the world have spent 40 years progressively removing the anonymity from the financial system to better fight crime and terrorism, only to have it returned by Nakamoto and his progeny. In this context, it does seem legitimate to ask if using cryptocurrencies should be its own trigger. Indeed, there is evidence that persons using cryptocurrencies as a form of payment may be doing so for nefarious ends. In their article *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, Sean Foley, Jonathan Karlsen and Tālis J. Putniņš, speculate that half the bitcoin market is engaged in illegal activity:

> "…approximately one-quarter of all users (25%) and close to half of bitcoin transactions (44%) are associated with illegal activity. Furthermore, approximately one fifth (20%) of the total dollar value of transactions and approximately one half-half of bitcoin holdings (51%) through time are associated with illegal activity."[16]

[14] "Guidance for a Risk-Based Approach to Virtual Currencies," Financial Action Task Force, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

[15] "SAR Stats: Technical Bulletin," Financial Crimes Enforcement Network, July 2014, https://www.fincen.gov/sites/default/files/sar_report/SAR_Stats_proof_2.pdf

[16] Sean Foley, Jonathan R. Karlsen and Tālis J. Putniņš, "Sex, Drugs and Bitcoin: How much illegal activity is financed through cryptocurrencies?" *SSRN*, January 2018, p. 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

However, for the purposes of AML risk there is an important distinction to be made between persons using cryptocurrencies as a form of payment, and those riding the wave of speculation. As Foley, et al., note, "…illegal users predominantly use bitcoin for payments, whereas legal users are more likely to treat bitcoin as an investment asset."[17] Persons purchasing cryptocurrencies as an investment would fall into a different risk profile than persons buying the same for the purposes of procurement. As a corollary, if the financial institution's client deals in cryptocurrencies, it should be ascertained if said dealings are for the purposes of exchange, fund movement or speculation, as each of these would present different levels of risk.

This risk can be further broken down by the coin in question, as there are certain cryptocurrencies (i.e., Dash, Zcoin) that were designed to get around the pseudo-anonymity of most cryptocurrencies and make it nearly, if not entirely, impossible to trace ownership. The use of such coins should prompt further questions from financial institutions as to the reason for using these specifically.

Cryptocurrencies and money laundering

Somewhat ironically, given the evident widespread use of cryptocurrencies to engage in predicate offenses, it does not appear to be a particularly attractive conduit for laundering money. The primary reason for this is the lack of widespread use of cryptocurrencies as a method of payment. As pointed out by Brenig, Accorsi and Muller in their article, *Economic Analysis of Cryptocurrency Backed Money Laundering*,

> "…limited acceptance currently has a direct effect on the execution of the ML process, providing negative incentives for money launderers to rely on cryptocurrencies. Even though this may evolve in the future, it is unlikely that they will gain greater acceptance than traditional financial instruments and services, which interact with a wide range of economic sectors."[18]

This sentiment was echoed by the FBI in a leaked, unclassified intelligence assessment, which states that the agency "assesses with low confidence, based on current user and vendor acceptance, that malicious actors will exploit Bitcoin to launder money."[19] While this assessment

[17] Ibid., p. 26.

[18] Rafael Accorsi, Christian Brenig and Gunter Muller, "Economic Analysis of Cryptocurrency Backed Money Laundering," AIS Electronic Library, 2015, http://aisel.aisnet.org/ecis2015_cr/20

[19] "(U) Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity," Federal Bureau of Investigation Directorate of Intelligence Cyber Intelligence Section and Criminal Intelligence Section, April 24, 2012, https://www.wired.com/ images_blogs/ threatlevel/2012/05/Bitcoin-FBI.pdf

CRYPTOCURRENCY TRANSACTIONS ARE FINAL AND NON-REVERSIBLE

was made in 2012, the lack of widespread user and vendor acceptance is still an issue with cryptocurrencies, and may be endemic in the blockchain's programming. As Dostov and Shust note succinctly,

> "There is little evidence, however, that bitcoin or any other cryptocurrencies have characteristics that will encourage massive adoption. Perceived anonymity is still a major attraction, but the upside is tremendous and publicly unacceptable risks of fraud, deception and high level of technicality. Clients spoilt by the $0 liability and purchase/buyer protection will be knocked back on their heels by the irreversibility of transactions. That will confine bitcoin to a limited number of evangelists, and [the] speculative market will eventually subside long before the last BTC will be mined in 2140."[20]

Put simply, rules protecting consumers from shady vendors in credit card and Automated Clearing House transactions, allowing for charge backs when services are not rendered or merchandise not provided, will no longer be applicable; cryptocurrency transactions are final and non-reversible. For these reasons, the general consumer has little incentive to adopt cryptocurrencies as a day-to-day payment method, and this lack of adoption by the wider public, in turn, makes these instruments less than attractive to people laundering money.

Extreme price volatility is another disincentive for use both as a payment method in the general population, and for those who would use cryptocurrencies for money laundering. For example, at its debut on the CME in mid-December 2017, bitcoin futures briefly surpassed $20,000, but fell to about half that price in less than a month's time, and continues to fluctuate rapidly, with a number of large market gaps, as shown on the CME chart in Figure 2. This volatility can be contrasted with the CME Eurodollar (see Figure 3) contract over the same period, which shows much less volatility.[21]

The listing of these products on major exchanges may ultimately result in less volatility, but the current market swings remain high, and can result in large changes to the value of bitcoin holdings. Criminals launder money so that they might enjoy their ill-gotten gains without the interference of law enforcement, so having the value of those gains slashed in half before they can be used is not a selling point.

In the money laundering cycle, cryptocurrencies would fall primarily into the placement stage. Nefarious actors complete their illegal deeds on the darknet, then move the proceeds of those transactions back to fiat currency as soon as practicable. It is for this reason that monitoring the gates to the financial system is so important when dealing with cryptocurrencies. Financial institutions who have clients regularly moving funds back and forth between exchanges should flag those accounts for additional monitoring.

What should be reported?

However, there remains a number of questions as to what should be reported on clients using cryptocurrencies. Aside from the transactions, client behavior and general demographics, the blockchain itself contains a wealth of information that may create obligations for reporting. The information in the blockchain is held in cryptographic format, but it is easily discernable with the right tools, which are freely available. Will financial institutions be obliged to scan the chain for recent transactions? If it is discovered that a client's coin was recently sent through a crypto-laundry, or a known darknet site, does the institution need to report that to law enforcement? If so, how far removed does this suspicious event need to be from the current block to be reportable? What if it is the last transaction before it reaches the institution, or five removed? How far back does one need to go? Are financial institutions obliged to scan client wallets to ascertain what kinds of coins are being held? For instance, if a client is holding a coin based on a zero-knowledge chain, which is designed to better protect the anonymity of the users, should this be reported? If they have the client's part of the chain, or private key, should the entire thing be reported?

Conclusion

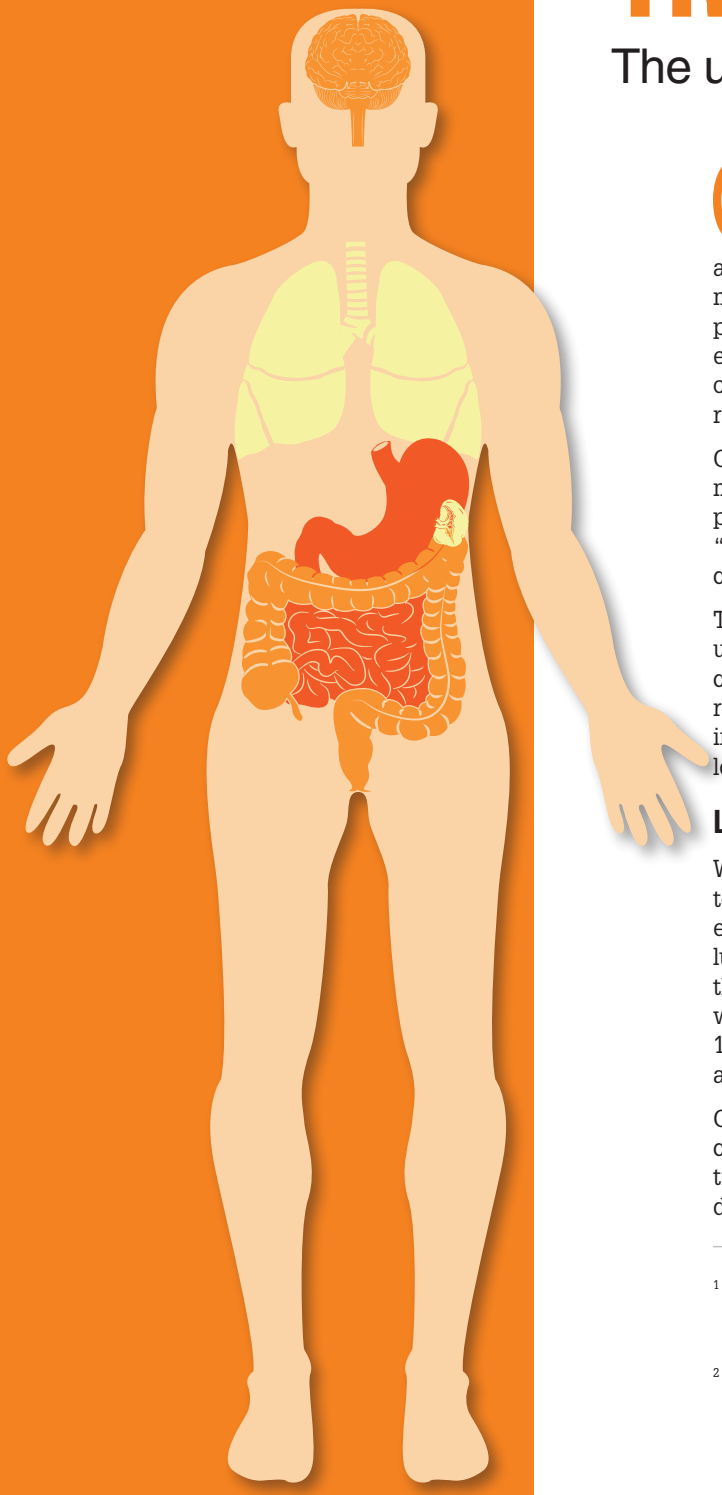
It is outside the scope of this article to answer these questions. The answers to these will come as regulators and law enforcement become increasingly familiar with cryptocurrencies and their enabler—the blockchain—and as user patterns become more apparent. Regulators are offering guidance piecemeal, and in very specific situations, in an apparent and well-founded attempt not to hinder the progress of a technology that will most likely change how the global financial system operates. In the interim, BSA officers whose institutions are exposed to these technologies will have to wrestle with the beasts on their own. While the intention of this article is to provide some assistance in that endeavor, like blockchain, it may be offering more questions than answers.

Chris Phillips, CAMS, VP, AML QA manager, Valley National Bank, Wayne, NJ, USA, cphillips@valleynationalbank.com

[20] Victor Dostov and Pavel Shust, "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?" Journal of Financial Crime, Vol. 21, No. 3, 2014, p. 259.

[21] Accessed May 2, 2018, CME BTC charts can be found at: http://www.cmegroup.com/trading/equity-index/us-index/bitcoin.html

Bank Secrecy Avenue



ORGAN TRAFFICKING:

The unseen form of human trafficking

Organ trafficking, a lucrative global illicit trade, is often a lesser discussed form of human trafficking among anti-human trafficking stakeholders due to its intricate and often stealth nature. Trafficking sex and/or labor are the more commonly thought of forms of human trafficking among public policy leaders and general awareness campaigns. However, organ trafficking holds a critical place with transnational organized crime groups due to high demand and relatively low rates of law enforcement.

Organ traffickers profit in the shadows, while their destructive medical footprint is the only thing that is felt. It leaves vulnerable populations, aka "donors," and first world beneficiaries, aka "recipients," open to severe exploitation and a lifetime of health consequences.

This form of illicit trade also leaves the private sector, in particular the financial industry, susceptible to being an unknowing conduit for its facilitation. Although, with the right training and raised awareness, financial institutions may play a pivotal role in unmasking organ traders by way of the financial trail they leave behind.

Low supply, high demand

When describing organ trafficking, there is often confusion as to how this crime can happen. Global Financial Integrity (GFI) estimates that 10 percent of all organ transplants including lungs, heart and liver, are done via trafficked organs.[1] However, the most prominent organs that are traded illicitly are kidneys, with the World Health Organization (WHO) estimating that 10,000 kidneys are traded on the black market worldwide annually, or more than one every hour.[2]

On their own, these numbers can be stark; however, when compared to average wait times for organs in developed countries, one can start to better understand the demand being diverted to black markets. In Canada, it is estimated that the

[1] "Transnational Crime and the Developing World," Global Financial Integrity, March 2017, http://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf

[2] Denis Campbell and Nicola Davison, "Illegal kidney trade booms as new organ is sold 'every hour,'" *The Guardian*, May 27, 2012, https://www.theguardian.com/world/2012/may/27/kidney-trade-illegal-operations-who

average wait time for a kidney is 4 years with some waiting as long as 7 years.[3] In the U.S., the average wait time for a kidney is 3.6 years according to the National Kidney Foundation.[4] In the U.K., wait times average 2 to 3 years but could be longer.[5]

Hiding in plain sight

Once obtained, trafficked organs can be transplanted to recipients in the most reputable of hospitals in major cities throughout the world but makeshift operating rooms in houses have often been the clandestine locations for such transplants.

Traffickers orchestrate the recruitment of the donor often from a place of vulnerability, and victims are not necessarily properly screened for their qualifications to be a healthy donor. Desperate patients in need of an organ may fall prey to a trafficker who could be posing as a "reputable" representative of an altruistic organ matching organization. Financial exploitation plays a key part in both sides of this scenario. In addition, organ traffickers could also be involved in other forms of human trafficking, such as sex and/or labor trafficking. Cases are emerging where an organ donor may have been a victim of sex trafficking and/or labor trafficking as well as a victim of organ trafficking, creating a multi-level equation of exploitation. The term "transplant tourism" is often utilized in describing this crime, as defined by the Declaration of Istanbul:

> "…travel for transplantation that involves organ trafficking and/or transplant commercialism or if the resources (organs, professionals and transplant centers) devoted to providing transplants to patients from outside a country undermine the country's ability to provide transplant services for its own population."[6]

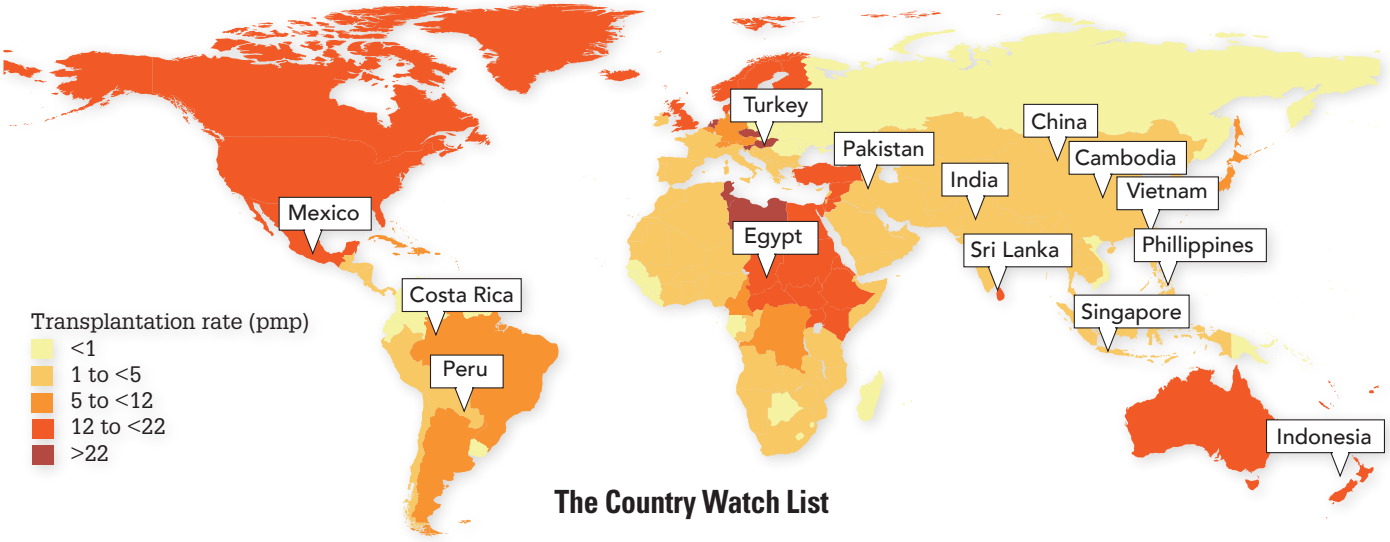
Expanding the human trafficking lexicon

How does organ trafficking fit within the broader definition of human trafficking? As stated in the Palermo Protocol of 2000, the basis for most national laws on human trafficking, organ trafficking is defined within the broader definition as:

> "Trafficking in persons' shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of

Figure A

Global distribution of living donor transplantation activity - 2017



Courtesy Jeremy Chapman

Data source: Global Observatory on Donation and Transplantation (www.transplant-observatory.org) slide courtesy of S. White

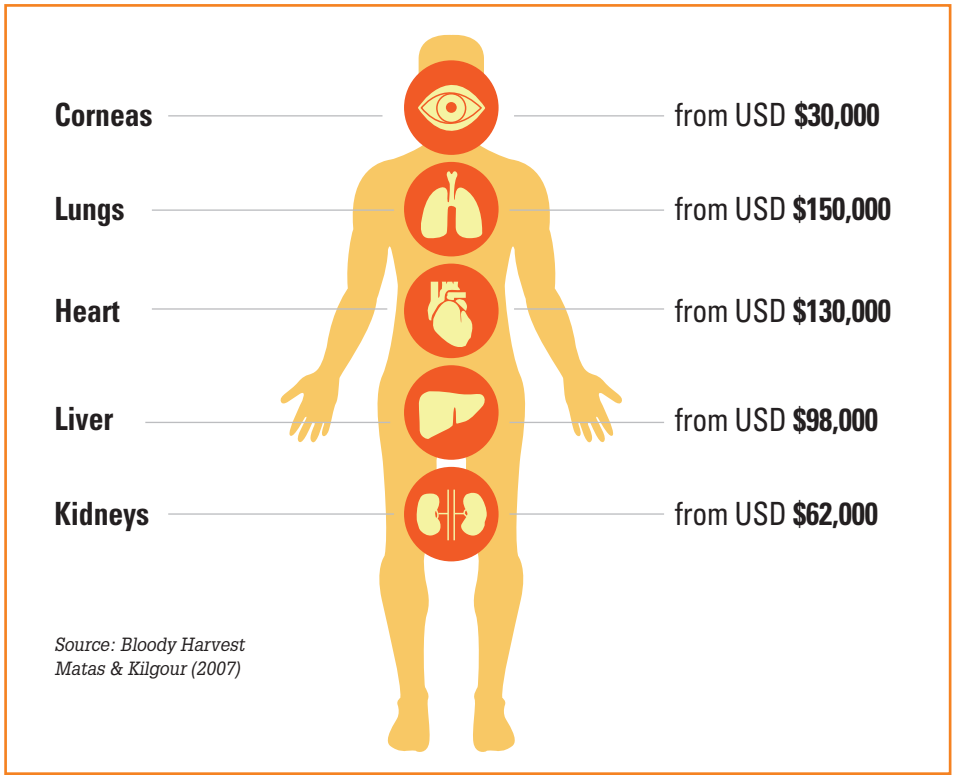
[3] "Organ Donation," The Kidney Foundation of Canada, https://www.kidney.ca/organ-donation

[4] "Organ Donation and Transplantation Statistics," National Kidney Foundation, https://www.kidney.org/news/newsroom/factsheets/Organ-Donation-and-Transplantation-Stats

[5] "Waiting list," NHS, October 14, 2015, https://www.nhs.uk/conditions/kidney-transplant/waiting-list/

[6] "The History and Development of the Declaration of Istanbul," Declaration of Istanbul on Organ Trafficking and Transplant Tourism, https://www.declarationofistanbul.org/about-the-declaration/history-and-development

Figure B



> payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs."[7]

In most countries, the buying and selling of organs is illegal (e.g., Iran is the only country in the world where buying and selling an organ is legal but this exception only applies to its citizens). Conversely, there are few laws that restrict an individual from leaving one's country to obtain an organ from someone abroad. In fact, there are many companies that cater to "transplant tourism" but purport to only match up recipients with donors who are willing.

It is difficult to know exactly how much transplant tourism generates annually worldwide but it is estimated that the illegal organ trade conservatively generates approximately $840 million to $1.7 billion annually, according to GFI.[8]

Unfortunately, even with estimated flow of funds crossing $1 billion annually, it is difficult for both law enforcement agents and anti-money laundering (AML) professionals to detect related financial activity. This is due to a myriad of factors such as a lack of domestic laws deterring citizens from travelling abroad, the transnational nature of the crime, and the savviness of the purveyors who know the laws related to organ trafficking well enough to circumvent them by way of shell companies and sanitized (legal) offerings via public websites.

Money laundering indicators

While it may be difficult for banks to detect financial transactions related to organ trafficking, it is not impossible as there are some indicators available. These red flags could include the following indicators and may be innocuous on their own but when combined, could present potentially suspicious behavior:

- Wire transfers to entities in high-risk jurisdictions (See Figure A) with names that include a variation of medical. For example, "Medicus"
- Methods of payment such as wires payment, email money transfer, and bulk cash withdrawal (See Figure B for estimated organ pricing)
- Payments between charities and medical tourism sites
- Credit card payments to travel agencies, airlines or hotels, prior to movement of money and travel
- First-line banking staff indication of potentially ill customers moving large amounts of funds to numbered companies or charities prior to travel
- Medical tourism websites that offer transplant services abroad that recommend utilizing their own trusted domestic doctors prior to traveling

One thing to keep in mind is that while traveling abroad to obtain an organ may be legal in certain countries, associated financial transactions would still be considered reportable in many jurisdictions as the act of purchasing an organ may be illegal within their country of citizenship. This stance gives AML professionals an interesting perspective above and beyond that of law enforcement as they are in a position to offer up intelligence that law enforcement agencies may have no insight on, nor a requirement to.

[7] "United Nations Convention Against Transnational Organized Crime and the Protocols Thereto" United Nations Office on Drugs and Crime, 2004, https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

[8] "Transnational Crime and the Developing World," Global Financial Integrity, March 2017, http://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf

Intelligence gathered by financial intelligence units (FIUs) within financial institutions associated with organ trafficking or transplant tourism can be further disseminated to international partners by national FIUs.

Project Protect expands: Project Organ

As previously stated, reporting on transactions related to organ trafficking is no easy feat. This way of raising awareness may prove to be an equally effective tool in deterring organ trafficking while increasing investigative knowledge toward reporting transactions.

One example of how awareness is being raised, within the context of AML and organ trafficking, is through the Project Protect initiative in Canada, launched by AML guru, Peter Warrack, in 2016. While initially designed to address sex trafficking, Project Protect was expanded to cover organ trafficking at the request of Dr. Francis L. Delmonico, M.D., professor of surgery at Harvard Medical School in 2018. The expansion is now known as "Project Organ" and its goals are similar to that of the original project, as it seeks to raise awareness and increase reporting to Canada's national FIU, the Financial Transactions and Reports Analysis Centre of Canada.

Looking forward

Countries like the U.S. and Canada did not include organ trafficking as a form of human trafficking when adopting their national laws on human trafficking. However, in the U.S. for example, some individual states like Massachusetts include organ trafficking within their state laws on human trafficking.

Since the Palermo Protocol, the public policy discourse of organ trafficking has been steadily gaining. In 2008, a group of key stakeholders in the global fight against organ trafficking convened to form the Declaration of Istanbul, which after Istanbul, created crucial new definitions around organ trafficking and transplant tourism, and developed promising practices to tackle the organ trade. Dr. Delmonico was one of co-founders of the Declaration of Istanbul and consequently, the Declaration of Istanbul Custodian Group (DICG), an international body tasked with implementing the principles of the Declaration. He said the following:

"The DICG has been an effective group of international colleagues monitoring illegal practices by their awareness of patients who return to their home country for sophisticated medical care following an organ transplant. Notifying the responsible authorities has led to the arrest of organ traffickers in Israel, China, Pakistan, India, Costa Rica, Egypt, and the United States."

In addition, the Council of Europe has adopted a Convention Against Trafficking in Human Organs in 2014 which recently went into effect in January of 2018.[9] This is a critical development as the first legal mechanism with a more universally agreed upon definition of organ trafficking.

More recent events, such as the February 2017 Summit on Organ Trafficking hosted by the Pontifical Academy of Sciences in Vatican City, have also shed light on the state of the organ trade.

As of today, the extent of organ trafficking is still unknown as to the number of such transplants performed annually. Furthermore, the full integration of the issue within the human trafficking field as a whole is still lacking.

In order to effectively combat organ trafficking and also raise its visibility among other forms of transnational organized crimes, it is vital to engage in effective public-private partnerships. The private sector, including the financial industry, can be essential in this global fight.

Christina Bain, director of the initiative on human trafficking and modern slavery, Babson College, Wellesley, Massachusetts, USA, cbain@babson.edu

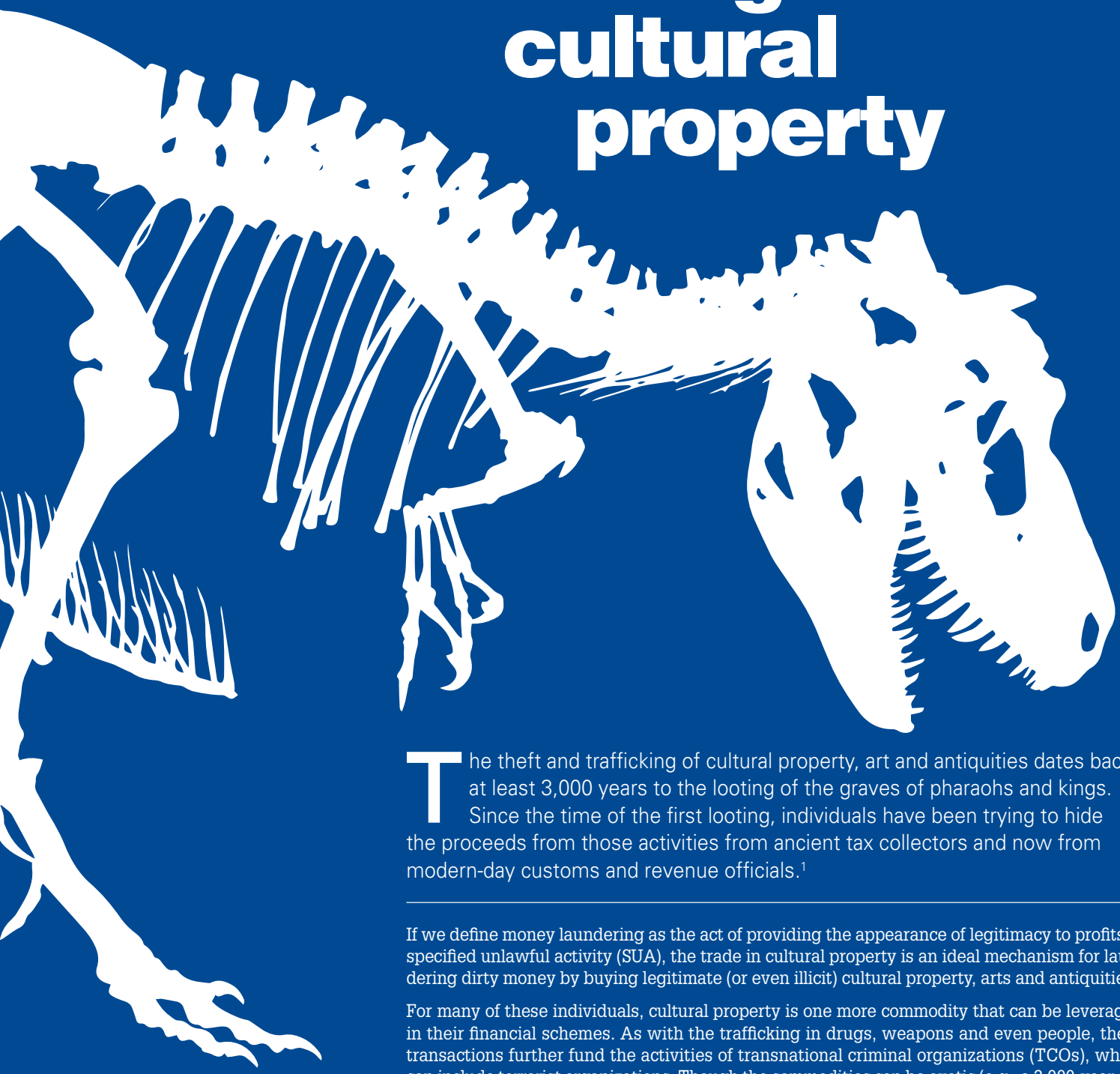
Joseph Mari, CAMS, senior manager of major investigations, Bank of Montreal, Toronto, Canada, joseph.mari@bmo.com

Advisor: Dr. Francis L. Delmonico, M.D., World Health Organization, advisory organ donation and transplantation and professor of surgery, Harvard Medical School, Massachusetts General Hospital, Boston, Massachusetts, USA, Francis_Delmomico@neds.org

Christina Bain, director of the initiative on human trafficking and modern slavery at Babson College, speaking on Project Organ and organ trafficking at an ACAMS Greater Toronto Chapter event in March 2018, as part of the expanded Project Protect mandate, hosted by Greater Toronto Chapter President Stuart Davis, chief AML officer at Bank of Montreal, and John Shoemaker, chief AML officer at Great-West Life of Manulife.

[9] "Trafficking in human organs: Council of Europe convention enters into force," Council of Europe, January 3, 2018, https://www.coe.int/en/web/cdpc/-/trafficking-in-human-organs-council-of-europe-convention-enters-into-force

Chasing cultural property



The theft and trafficking of cultural property, art and antiquities dates back at least 3,000 years to the looting of the graves of pharaohs and kings. Since the time of the first looting, individuals have been trying to hide the proceeds from those activities from ancient tax collectors and now from modern-day customs and revenue officials.[1]

If we define money laundering as the act of providing the appearance of legitimacy to profits of specified unlawful activity (SUA), the trade in cultural property is an ideal mechanism for laundering dirty money by buying legitimate (or even illicit) cultural property, arts and antiquities.

For many of these individuals, cultural property is one more commodity that can be leveraged in their financial schemes. As with the trafficking in drugs, weapons and even people, these transactions further fund the activities of transnational criminal organizations (TCOs), which can include terrorist organizations. Though the commodities can be exotic (e.g., a 3,000-year-old mummified hand, a 115-million-year-old microraptor fossil, a $10-million-dollar painting), the techniques used to investigate these cases are often those learned from investigating transnational crimes that include money laundering.

▲ *"Hannibal," by Jean-Michel Basquiat. New York, New York: June 17, 2015, inside 1 St. Andrew's Plaza, office of the U.S. Attorney for the Southern District of New York, Preet Bharara, officiates over a repatriation ceremony that returns a painting, "Hannibal," by Jean-Michel Basquiat, to its rightful owners in Brazil. Photo Credit: JB NICHOLAS / Splash News.*

U.S. Immigration and Customs Enforcement/Homeland Security Investigations (HSI) is the largest investigative agency within the U.S. Department of Homeland Security (DHS). HSI investigates and enforces more than 400 federal criminal statutes to include the Immigration and Nationality Act (Title 8), U.S. Customs laws (Title 19), General Federal Crimes (Title 18) and the Controlled Substances Act (Title 21). HSI special agents use these authorities to investigate all types of cross-border criminal activity and closely coordinate with U.S. Customs and Border Protection (CBP), as well as other federal, state and local law enforcement agencies in a unified effort to target TCOs involved in criminal activity including the looting and illegal import of cultural property, arts and antiquities into the U.S.

When it comes to cultural property trafficking, the level of cooperation among law enforcement agencies has grown substantially at the national level; we are now working together to develop and deliver integrated training on this issue. HSI also works closely with the financial industry on both individual cases as well as on identifying broader trends, indicators and typologies. Our goal, as we move forward, is to build upon the good relationships we have developed over the years in this program, and integrate it into our larger anti-money laundering (AML) engagement with the financial industry, thus institutionalizing and broadening our efforts to identify and stop this illicit activity while continuing our mission to protect our critical financial infrastructure.

HSI brings many years of experience and expertise in combating money laundering. "Every criminal case HSI investigates, regardless of category, has a financial nexus. HSI seeks to identify not only the illicit proceeds of crime but also targets the financial networks and third-party facilitators."[2] The Illicit Finance and Proceeds of Crime Unit (IFPCU) develops investigative techniques and typologies to close vulnerabilities in the U.S. financial system and criminally pursue violators of financial crimes. The IFPCU forges partnerships with other government agencies as well as public and private sector entities to enhance AML initiatives, as well as provides AML assessments, training, and best practices in the fight against global money laundering.

[1] For the purposes of this article, cultural property is defined by the United National Educational, Scientific and Cultural Organization (UNESCO) as tangible cultural heritage. Movable cultural heritage includes painting, sculptures, coins and manuscripts; immovable cultural heritage includes monuments, archaeological sites, and so on.

[2] "Homeland Security Investigations," U.S. Embassy in Singapore, January, 19, 2016, https://sg.usembassy.gov/wp-content/uploads/sites/197/2015/07/HSI_Placemat.pdf

ICE/HSI's role in cultural property investigations

It may seem counterintuitive that an agency associated with investigating immigration violations is charged with investigating cultural property trafficking. However, in 2003, HSI was the product of merging customs authorities and capabilities from the U.S. Department of the Treasury with immigration authorities and capabilities from the U.S. Department of Justice. U.S. federal importation laws regarding smuggling and trafficking of any commodity, based on customs authorities, provide HSI special agents the authority, jurisdiction and responsibility to take the leading role in criminal investigations that involve the illicit importation and distribution of stolen or looted cultural property and prosecuting those responsible for these crimes. Simply put, HSI has the capability to investigate these cases based on its customs and border authorities. To help oversee this area, HSI has established the Cultural Property, Art and Antiquities Program (CPAA), which supports investigations involving the trafficking of cultural property from countries around the world; trains law enforcement in the handling, investigation and prosecution of these cases; and ultimately facilitates the repatriation of these objects to their rightful owners.

Through its international and domestic footprint, HSI special agents partner with federal, state and local agencies, private institutions and foreign governments to conduct these often complex investigations.

The import violations and seizure/forfeiture authorities described in sections 18 and 19 of the U.S. Code are usually the laws HSI uses to initiate a cultural property investigation. However, fact patterns may cause an agent to investigate further and find an indicator or nexus to financial crimes, a charge that, as mentioned above, HSI pursues in every criminal programmatic area that HSI investigates.

PEOPLE ATTEMPTING TO CONCEAL CONTRABAND OR ILLEGALLY OBTAINED CULTURAL PROPERTY LIE TO CUSTOMS OFFICERS TO EVADE DETECTION

Examples of the nexus between cultural property trafficking and money laundering

There are three main areas where HSI is exploring the nexus between money laundering and the trafficking of cultural property as a means of furthering investigations and increasing the likelihood of criminal prosecutions:

1. The proceeds of trafficking cultural property are often used to further the activity. Federal importation laws related to smuggling are a specified unlawful activity (SUA) under federal money laundering statutes. As noted above, smuggling laws are the bread and butter for HSI special agents initiating cultural property cases. People attempting to conceal contraband or illegally obtained cultural property lie to customs officers to evade detection. They do not report the items at all or they misidentify the artifact because of its country of origin. Sometimes they are caught, but not always. When they are not, they may be able to sell their Pre-Columbian pottery or their dinosaur fossils from abroad within the U.S. Then the criminal uses the proceeds of that sale to purchase more illicit antiquities and continue the cycle.

   For example, in 2013, HSI repatriated dinosaur fossils, including a complete Tyrannosaurus Bataar skeleton, to Mongolia that had been forfeited by a self-described commercial paleontologist who bought and sold whole and partial fossilized dinosaur skeletons. Between 2010 and 2012, the defendant "acquired dinosaur fossils from foreign countries and unlawfully transported them to the U.S., misrepresenting the contents of shipments on customs forms. Many of the fossils were unlawfully taken from Mongolia in violation of Mongolian laws declaring dinosaur fossils to be the property of the Government of Mongolia, and criminalizing their export from the country."[3]

   The investigation revealed the Tyrannosaurus Bataar skeleton and others were smuggled through China and Great Britain to "the United States, using false or misleading statements on customs forms concerning their identity, origin, and value."[4] The defendant then sold or attempted to sell these fossils to others. With the proceeds, he purchased additional illicitly obtained fossils, paid for smuggling costs and built an elaborate compound at his Florida residence. His compound included a 5,000-square-foot warehouse that was used to restore and prepare the fossils for sale.

2. If the importation of illicit cultural property is an SUA, and the seller of that cultural property sends the proceeds of that sale to a foreign location, the international transfer of those funds is money laundering. The overwhelming preponderance of cultural property smuggled or brought into the U.S., contrary to law, is from another country. It stands to reason that someone trading in international cultural property may send the proceeds of those transactions internationally, if only, as noted above, to continue to further their activities. The funds may pay looters who are digging up artifacts or objects from the ground. The funds may also be used to pay brokers working in specific countries to transport goods from conflict zones across transit countries to reach a dealer and eventual buyer in the U.S., in China or in the U.K.—three of the largest destination countries for both licit and illicit cultural

[3] "Florida Man pleads guilty in New York to smuggling dinosaur fossils," U.S. Immigration and Customs Enforcement, December 28, 2012, https://www.ice.gov/news/releases/florida-man-pleads-guilty-new-york-smuggling-dinosaur-fossils

[4] Ibid.

property. In addition, a red flag in one of these cases may be that the artifacts are from a conflict zone.

Using the same case example from above, the defendant in the Tyrannosaurus Bataar case sent money to a collaborator in England and to an individual in Mongolia who procured the fossils, thus laundering money through the international transfer of funds.

3. If an individual or organization spends the proceeds of an SUA on licit or illicit goods, money laundering occurs. In 2017, the U.S. attorney for the Southern District of New York and HSI's Boston office announced the return of 95 works of art to the judicial administrator of Banco Santos' bankruptcy estates. These artworks, which once belonged to Brazilian banker Edemar Cid Ferreira, were seized as part of the assets that Ferreira, his associates and family had purchased with funds from Banco Santos that were unlawfully obtained. Many of these works had been smuggled out of Brazil and into the U.S. and Europe. Several other works entered the U.S. illegally, including ones by Jean-Michel Basquiat (see below) and Roy Lichtenstein as well as an ancient Roman statue (see right). In this scenario, the proceeds of an SUA were used to purchase licit art, thus money laundering took place. Coincidentally, because the licit art was then smuggled into the U.S., the case followed the familiar pattern of a cultural property case.

It is worth noting an additional scenario that is untried in courts, but has been helpful in "encouraging" some institutions to forfeit art and artifacts that were obtained, either by them or their seller/donor, illegally.

> IF AN INDIVIDUAL OR ORGANIZATION SPENDS THE PROCEEDS OF AN SUA ON LICIT OR ILLICIT GOODS, MONEY LAUNDERING OCCURS

If an institution knowingly exhibits an example of illicit CPAA in its collection and accepts money from visitors wishing to access the site or view the collection, the institution could be engaging in money laundering. Theoretically, because the institution may be in violation of 18 USC 2315, which deals with possession of stolen merchandise worth more than $5,000 brought illegally into the U.S., any monies received by the institution while that piece was on display would be proceeds of a specified unlawful activity—the 18 USC 2315 violation—under the money laundering statutes. Accordingly, the institution could be charged with receiving and using that money in furtherance of a crime. Notably, the patron does not even have to view the illicit painting or artwork; giving the patron access to the institution in which the painting is displayed may be enough to make any entrance fee the illicit proceeds of the crime of possession of stolen property.

Conclusion

Financial crimes, especially money laundering, are key components of HSI's cultural property investigations. HSI is training special agents to consider these areas when seeking prosecutions in what can otherwise seem to be somewhat niche cases. For example, many of the indicators of money laundering for cultural property are similar to indicators for any commodity:

- Commodities are over- or under-valued;
- Artifacts are shipped from areas of conflict and civil unrest;
- Payments are made to a vendor by an unrelated third party;
- Commodities are being traded that do not match the vendor involved; and
- There is a sudden change in company name and ownership yet the business model remains the same.

As HSI broadens its attempts to mitigate the trafficking of cultural property, the agency will continue to use the proven techniques of financial crimes investigators that have served so well in the past.

Raymond Villanueva, assistant director, ICE/HSI/International Operations, Washington, D.C., USA

Mary E. Cook, national program manager, Cultural Property, Art and Antiquities Program, ICE/HSI/International Operations, Washington, D.C., USA, Mary.E.Cook@ice.dhs.gov

Cultural Property Walk

Real considerations for law enforcement in seizing virtual currency

Myths continue to girdle virtual (crypto) currencies, including that they are anonymous and exclusively used by criminals to purchase items on the darknet or to launder money. Bitcoin is most commonly associated with these myths, despite the fact that it is not anonymous, but rather pseudonymous, and like cash, it is used by criminals, but not exclusively.

Such misunderstandings are unhelpful, and dangerous from a law enforcement perspective. To focus on Bitcoin and ignore privacy coins, such as Monero, Zcash and Dash, means missed opportunities for law enforcement when conducting investigations and seizing the assets of criminals in searches.

Even with some knowledge about virtual currencies, law enforcement can miss opportunities for seizure and expose virtual assets seized to loss as in the case of the first seizure of bitcoins in Canada in 2014 as explained below.

During the search of an online drug and firearms dealer in Toronto, the suspect informed the police officer that he had transacted in bitcoins, and provided the details of his web wallet and keys. The quick-thinking officer opened a wallet on his own phone and transferred the bitcoins to his mobile wallet from the suspect's web wallet on his computer. Subsequently, the police opened a wallet on an online exchange where they transferred the custody of the coins from the officer's phone and where the 288 seized coins currently remain. When seized, the coins were worth $88,000; today they are worth $3.2 million, as legal wrangling continues concerning issues of paying legal fees.

Similarly, in March 2017, Toronto police seized $30,000 in bitcoins and transferred them to an online exchange wallet. Both seizures remain on "hot" wallets, vulnerable to being stolen by hackers or others depending on how secure the private keys are stored. This is not good practice.

These two examples demonstrate the need to raise awareness of virtual currencies within law enforcement generally, but also with those charged with the custody of seized assets and with the prosecution of criminal charges.

Recently, when discussing the results of a search in a fraud investigation with a police officer (it was known the suspects moved their illicit funds using virtual currency), it was learned that false identity documents were discovered together with computers and smartphones.

When asked if virtual currency wallets had been found on the devices, the officer said that the results from forensics would take months to be known. The officer was unaware of deterministic wallets, (that can be recreated typically using a 12 or 24-word back-up phrase or word sequence), and the likelihood that any virtual funds that did exist would be long gone by the time the forensic report was received, (i.e., a missed opportunity).

Despite increasing requests from law enforcement to receive training on virtual currencies from municipal, provincial and federal agencies, many in law enforcement (at least in Canada) have a limited knowledge of virtual currency. The purpose of this article is to provide practical information to law enforcement colleagues that can be used immediately and to build a foundation to learn more.

Virtual currency basics

Virtual currencies exist as data entries on, in the case of Bitcoin, a publicly accessible online database called a blockchain. The entries (records of transactions in blocks, similar to each page of a traditional ledger) are secured using cryptography meaning that the entries are extremely difficult to change.

In the case of Bitcoin, the transaction records include the amount (in bitcoins), and the Bitcoin address they were received from, sent to and currently remain. Therefore, Bitcoin transactions are not anonymous. However, the ownership of the wallets is anonymous, at least publicly; hence the term pseudonymous.

Wallets created through an exchange, for example, will often require supporting identity documentation, such as a copy of a driver's license, passport or utility bill, and many exchange wallets are linked to real bank accounts, credit or debit cards. Depending on the jurisdiction, this information may be available to law enforcement upon service of a warrant, production order or subpoena.

Wallets, which hold the public and private keys required to receive and spend bitcoins (or other virtual currencies), are available on different platforms, including desktops, web wallets (hosted by an exchange of external provider), mobile wallets (on a smartphone), paper wallets and hardware wallets.

As previously mentioned, regardless of the type of wallet, if the wallet can be recreated using a backup seed, then wallets seized by law enforcement are at risk of having their funds transferred out of law enforcement's reach.

Wallets

Web, desktop and smartphone wallets either require the user to download an app or login to the website of the wallet provider. Some common apps are Mycelium and Bitcoin wallet. Online wallets may appear on a suspect's desktop or under favorites on their computer, so during searches law enforcement should be aware of these.

Various types of wallets exist—some are designed to transact solely in bitcoins and others in multiple currencies. Some wallets, such as Jaxx, allow conversion between one virtual currency to another, (e.g., Bitcoin to Litecoin) within the wallet's app. A list of the various types of wallets can be found on bitcoinwiki.[1]

In addition to wallets law enforcement may encounter on electronic devices, officers should also be looking for hardware wallets, which often have the appearance of a USB stick. Examples of hardware wallets include Ledger Nano wallets, TREZOR wallets and KeepKey wallets.

Hardware wallets allow their owners to keep their virtual currency holdings offline. If the physical wallet is lost, becomes defective or is seized by law enforcement, a new wallet can be ordered and recreated using the backup seed.

Hardware wallets are ideally suited for use by law enforcement when conducting searches and seizing virtual currencies as long as the appropriate safeguards are in place to prevent unauthorized access to the wallet (and its backup seed).

Similarly, law enforcement should be alert to the existence of paper wallets, literally a piece of paper on which is printed the wallet address (to receive virtual currency) and the private key, which is used to spend or transfer the wallet contents. An example of a paper wallet is shown below:

In reality, the writing on the wallet shown is not actually required. Merely keeping a copy of the two QR scan codes will suffice to be able to access any available funds associated with the public address.

Astute readers may realize that a paper wallet performs the same function as a bearer share, identified many years ago as being a money laundering risk. The person in possession of the paper owns the shares, or in this example, the virtual currency.

[1] "Cryptocurrency wallets list," bitcoin wiki, February 23, 2018, https://en.bitcoinwiki.org/wiki/Cryptocurrency_wallets_list

Technology

As history has demonstrated, lawmakers are always playing catch-up. Technology presents possibly the best example of how quickly and significantly, our laws tend to lag behind. How law enforcement has dealt with new and emerging technologies and has remained constant. As criminals utilize technologies to commit crimes, officers try to keep up the pace by "making the best decision possible." Without a solid platform of law upon which to base their actions, officers are left "doing the right thing for the right reasons" as in the case of the first bitcoin seizure in Toronto. Such investigative decisions are then scrutinized for years through the levels of the courts, until eventually some direction or guidance is provided through case law.

Thinking back to the not-so-distant past, cell phones presented (and now smartphones still present) a challenge for law enforcement (e.g., to retrieve data or gain access to the encrypted contents).

In the early years of cell phones (the 1970s), officers would routinely search the content of an arrested individual's cell phone, document any evidence found therein and utilize that evidence as they saw fit. But it took 40 years in Canada for guidance on the search and seizure of cell phones in the form of a landmark ruling by the Canadian Supreme Court, R v. Fearon.[2]

R v. Fearon laid out four specific criteria that would allow for a warrantless search of a cell phone. If the seizure did not fall within those specific criteria, judicial authorization was required to conduct such a search.

Virtual currencies represent the new technology challenges for law enforcement. Criminal statutes (and law enforcement procedures) in this space lag behind the technology and its use by criminals, with the result that officers are utilizing the "make the best decision possible" approach to seizing virtual currencies. At a minimum, the key to "making the best decision" is to have a working understanding of virtual currencies, what they look like and what they represent.

Any officer seeking to seize virtual currencies will have to answer a number of questions:

- Is virtual currency money?
- Do they fall within the definition of property?
- Does the ability to seek judicial authorization to seize proceeds of crime include virtual currencies?
- Is there any avenue to actually seize a virtual wallet?
- What form should the management of seized virtual currencies take?

Are virtual currencies money?

Canadian laws were not written with a view to seizing and forfeiting virtual currencies. There is currently no predominate legal definition of money that includes virtual currencies. However, a recent court ruling may provide law enforcement guidance, at least in the U.S. In May 2017, Florida incorporated virtual currencies into the Florida Money Laundering Act. The lawmakers classified virtual currencies as a "monetary instrument" and further defined it as a "medium of exchange in electronic or digital format that is not a coin or currency of the United States or any other country."[3]

Japan passed the Virtual Currency Act in March 2017. The act recognized virtual currencies as a form of payment method but fell short of recognizing it as a legally recognized currency or legal tender.

Although these acts are not binding outside of their specific jurisdictions, they may provide some guidance to law enforcement officers who are attempting to justify the seizure of or obtain a warrant for the seizure of virtual currencies.

Can cryptocurrencies be considered proceeds of crime?

In Canada, proceeds of crime is defined as "Any property benefit or advantage obtained directly or indirectly"[4] by the commission of a for-profit serious offense. Given the broad definition of a "proceed of crime," in the Canadian context an educated argument could be made to justify the seizing of virtual currencies as such.

Do the conventional methods of seizing the proceeds of crime fit?

Most common law jurisdictions have similar search and seizure laws. When seizing personal (tangible) property, law enforcement typically requires obtaining judicial authorization prior to seizing assets as proceeds of crime. There are certain exceptions to this rule but the general rule of law is that all seizures require judicial oversight. When seizing "real" (intangible) property, the need to obtain prior judicial authorization is even greater. A large number of financial institutions will not freeze accounts and land registry offices will not register a restraint without judicial authorization.

The fact that virtual currencies wallets can be found in several different mediums, such as online wallets, USB keys and even paper wallets, presents an even bigger challenge to law enforcement's ability to seize virtual currencies.

Crossing international borders in "possession" of virtual currency is a developing challenge for law enforcement and customs

[2] R v. Fearon, 2014 SCC 77, [2014] S.C.R. 621.

[3] Brad Gershel and Marjorie J. Peerce, "Florida Lawmakers Seek to Bring Virtual Currency into the Fold," *Money Laundering Watch*, April 25, 2017, https://www.moneylaunderingwatchblog.com/2017/04/florida-lawmakers-seek-bring-virtual-currency-fold/

[4] The definition on the Canadian Criminal code speak to indictable offenses, but for the purpose of this article the wording "for profit serious offense" is more effective.

[5] Landon Mutch, "U.S. Senate Bill S.1241 to Criminalize Concealed Ownership of Bitcoin," *BTCMANAGER*, December 1, 2017, https://btcmanager.com/us-senate-bill-s-1241-criminalize-concealed-ownership-bitcoin/

officers. Bill S.1241 currently before the U.S. Senate[5] seeks to criminalize concealed bitcoin ownership (i.e., undeclared bitcoin or other virtual currencies).

Asset management

There is a saying in law enforcement that says: "If it has to be fed, don't seize it!" Although this saying is not entirely accurate, it does serve as a useful reminder to officers that the responsibility of managing, storing or in some cases feeding seized property lies with the state. Given the volatile nature of virtual currencies, having sound policies in place surrounding the management of them is therefore essential. The fact that the seized bitcoins remain on a hot exchange wallet liable to be hacked, is troubling.

It is important to remember that at the time of seizure, the accused has not been found guilty nor has there been a forfeiture order for the seized "property." As such, it is incumbent on the state to manage that property effectively to ensure it does not depreciate.

At the time of the Toronto seizure, the value of the bitcoins was approximately CA$88,000; given the current price of Bitcoin, the decision to not convert the coins to fiat currency appears a sound one. But what if the seizure had taken place on December 17, 2017, when Bitcoin was at an all-time high? What if in September 2018, all the charges against the accused are dropped and the bitcoins are ordered to be returned; is the state now liable for the change in value since the seizure?

If a prosecution is successful, and the seized virtual assets are ordered by a court to be liquidated, what is the process to do that? The U.S. provides recent precedent in the auction of 3,813 bitcoins by the U.S. Marshals Service in January 2018.[6] The Bulgarian government, who holds more than 200,000 bitcoins seized as the proceeds of crime, may wish to follow the U.S. precedent, seeing as how these bitcoin are valued in the billions of dollars.[7] Hopefully, they are not still sitting on an exchange!

Legal costs

In Canada, accused persons can apply to use the seized proceeds of crime to pay for a legal defense. This begs the question as to whether accused persons can apply for seized virtual currencies to be used in the same way to pay for their legal defense. Under current Canadian law, the legal answer from most learned Crown Counsel would be "No!" However, applications can still be made and judiciary, who are looking to update laws, have the ability to rule as they see fit.

If a court directs that seized virtual currency can be used to pay legal costs, questions will arise about whether the full amount of currency is converted to fiat, or just enough to pay for the legal costs.

However, current Canadian legislation does allow an order forcing an accused to pay back proceeds of crime that have been used to fund a legal defense. Under the Fine In Lieu of Forfeiture provisions of the Canadian Criminal Code the accused, upon conviction, can be ordered to pay back monies (i.e., virtual currencies) that have been used to pay their defense bill; this of course begs the questions, "In fiat or virtual currency, and what if the price of virtual currency had dropped or risen over the period?"

Articulation

Law enforcement's ability to articulate the rationale behind their course of action is critical and can make or break a case. The expectation of our law enforcement officers is that they are better educated now than at any time in history. It is reasonable to assume that most seizures of virtual currencies will occur during a search incident to arrest or under exigent circumstances. Search incidents to arrest or exigent circumstances seizures demand strong and clear articulable grounds.

Any officer who has an expectation to seize virtual currencies in relation to exigent circumstances needs to have a working understanding of such currencies. Law enforcement does not need to be experts in hashing, nodes and miners, but they should be expected to have a good understanding of how virtual currencies are transferred and how they can be stored, if they expect to have any success in seizure and subsequent forfeiture.

As was the case when cell phones were first introduced in 1970s education, emerging technologies is, and always will be, law enforcement's best friend.

Summary

The bottom line for law enforcement is that they cannot seize virtual currency if they do not recognize it and do not know where to look. Even if evidence of virtual currency is found, unless law enforcement is equipped with the knowledge and the tools to take secure possession of it, then it will not happen and criminals will keep their ill-gotten gains.

Knowledge comes from education and associations, such as the Association of Certified Anti-Money Laundering Specialists, who can assist with this and play an important part in protecting the financial system, albeit in the "virtual space."

Dwayne King, CAMS-FCI, CFCS, CBP, AML manager, TD Bank Group, Toronto, Ontario, Canada, dwayne.king@td.com

Peter Warrack, CAMS, CBP, CFE, chief compliance officer, Bitfinex, peter.warrack@bitfinex.com

Disclaimer: The opinions expressed in this article are those of the authors and should not be construed as reflecting those of their employers. In addition, the knowledge contained in this article was obtained by Dwayne King outside of his role with TD Bank Group.

[6] "For Sale Approximately 3,813.0481965 Bitcoins," U.S. Marshals Service, https://www.usmarshals.gov/assets/2018/bitcoinauction/

[7] Nikhilesh De, "The Bulgarian Government Is Sitting on $3 Billion in Bitcoin," *CoinDesk*, December, 1, 2017, https://www.coindesk.com/bulgarian-government-sitting-3-billion-bitcoin

CHALLENGES AND BEST PRACTICES SURROUNDING THE BSA/AML INDEPENDENT REVIEWS

Issues involving the independent reviews of Bank Secrecy Act/anti-money laundering (BSA/AML) were amongst the most frequently cited BSA/AML examination findings for community banking organizations by the Richmond Federal Reserve from 2014 to mid-2017. The independent review issues were centered in two primary areas: (1) transaction testing was not performed to validate suspicious activity monitoring processes, and (2) the integrity and accuracy of management information systems (MIS) used in the BSA/AML compliance program was not assessed. This article focuses on expectations around transaction testing and ensuring an appropriate independent review scope.

Risk-based transaction testing and the independent review

The expectation is that risk-based transaction testing be performed as part of the independent review process to ensure that suspicious activity monitoring processes are working as intended. Transaction testing for suspicious activity means that the independent reviewer will select a sample of customer accounts that include transactions that may appear suspicious, unusual or outside of the customer's expected activity and then determine if the bank identified the same potentially suspicious activity. When transaction testing, the reviewer may evaluate the documentation associated with the customer's account, including customer due diligence information and previous transaction history, to help understand and evaluate the bank's suspicious activity report (SAR) decision-making process. Ultimately, the point of the transaction testing is to assess whether the institution's suspicious activity monitoring processes are identifying the suspicious activity and if so, whether the activity is being reported to FinCEN. In some cases, testing results from independent reviews of MIS used to identify suspicious activity can also be relied upon to help gauge the effectiveness of suspicious activity monitoring processes.

The independent reviewer may select transactions from various sources including, but not limited to, wire logs, SAR referral forms completed by branch personnel and automated system output such as alerts and reports generated from the core processor to monitor suspicious activity, such as a large currency transaction report. For example, a specific transaction the reviewer might select from a large currency transaction report could be a large cash transaction inconsistent with the expected activity of the account holder. The reviewer may also select wire transfers to transaction test for suspicious activity. Some reasons to select a specific wire transaction may be because the wire is for a high dollar amount and/or has been sent to a country identified as high risk for BSA/AML. The scope of the testing should be representative of the risk within the portfolio.

Independent testing challenges from the banker's perspective

Ensuring that transaction testing for suspicious activity monitoring was in scope for the independent test did not appear to be a problem for the bankers interviewed for this article but they faced other challenges. Joe Soniat, vice president and BSA/AML officer of Union Bank and Trust, a nearly $14 billion bank headquartered in Richmond, Virginia, suggested that his biggest challenge has been the knowledge level of individuals performing the independent review. He recommends taking a hard look at the reviewers' resumes and having a conversation before engaging them. Another anti-money laundering (AML) professional, Heather Allen, first vice president and Bank Secrecy Act (BSA) officer of the billion-dollar Peoples Bank NC headquartered in Newton, North Carolina, stated that her biggest challenge with the independent test was "ensuring that the scope

> THE SCOPE OF THE TESTING SHOULD BE REPRESENTATIVE OF THE RISK WITHIN THE PORTFOLIO

of the independent test is specific to my bank and is sufficiently deep enough to test my controls." Ms. Allen's portfolio includes a number of money services businesses (MSBs) and she has found that being explicit about the portfolio at the outset of the engagement with the auditors is helpful in setting an appropriate independent review scope. An executive vice president and director of AML compliance at South State Bank, headquartered in Columbia, South Carolina, said that one of her challenges was auditors not understanding the organization from a BSA/AML risk exposure standpoint nor the risk implications of products or services offered by her bank.

Best practices

To help ensure that you are meeting expectations relative to the independent review of suspicious activity processes, consider the following:

- Consider what the independent reviewer will be doing to assess your process for identifying and reporting suspicious activity. Although you may not always be in the position to dictate exactly what the scope of your independent review will be because it is "independent," assure yourself that the scope includes transaction testing for suspicious activity or for any area for which you need an in-depth review. For example, if you have a large portfolio of MSBs like Ms. Allen, try to ensure that testing and a review of controls surrounding them is included in the scope of the review.
- Request time with the auditors up front. "I find that a detailed conversation about my BSA program and its policies/procedures, customer base, risk assessment, products/services, and geographic and other risks really helps to set the stage for the auditors and gives them needed context for the scope and review," said South State Bank's Robertson.
- Use the *Federal Financial Institutions Examination Council's Bank Secrecy Act/Anti-Money Laundering Examination Manual*, which includes independent testing minimums and examination procedures, as a guide to a sufficient scope of the BSA independent review in general and specifically as it relates to transaction testing. This section of the manual suggests that the independent review should include "a review of the effectiveness of the suspicious activity monitoring systems and the overall process for identifying and reporting suspicious activity as well as appropriate risk-based transaction testing."[1] Also, use your BSA/AML risk assessment and previous independent review report and results to help set the scope.
- Understand that the independent review can be conducted by someone working within your organization or an outside party. The independence and qualifications of the reviewer are the key.

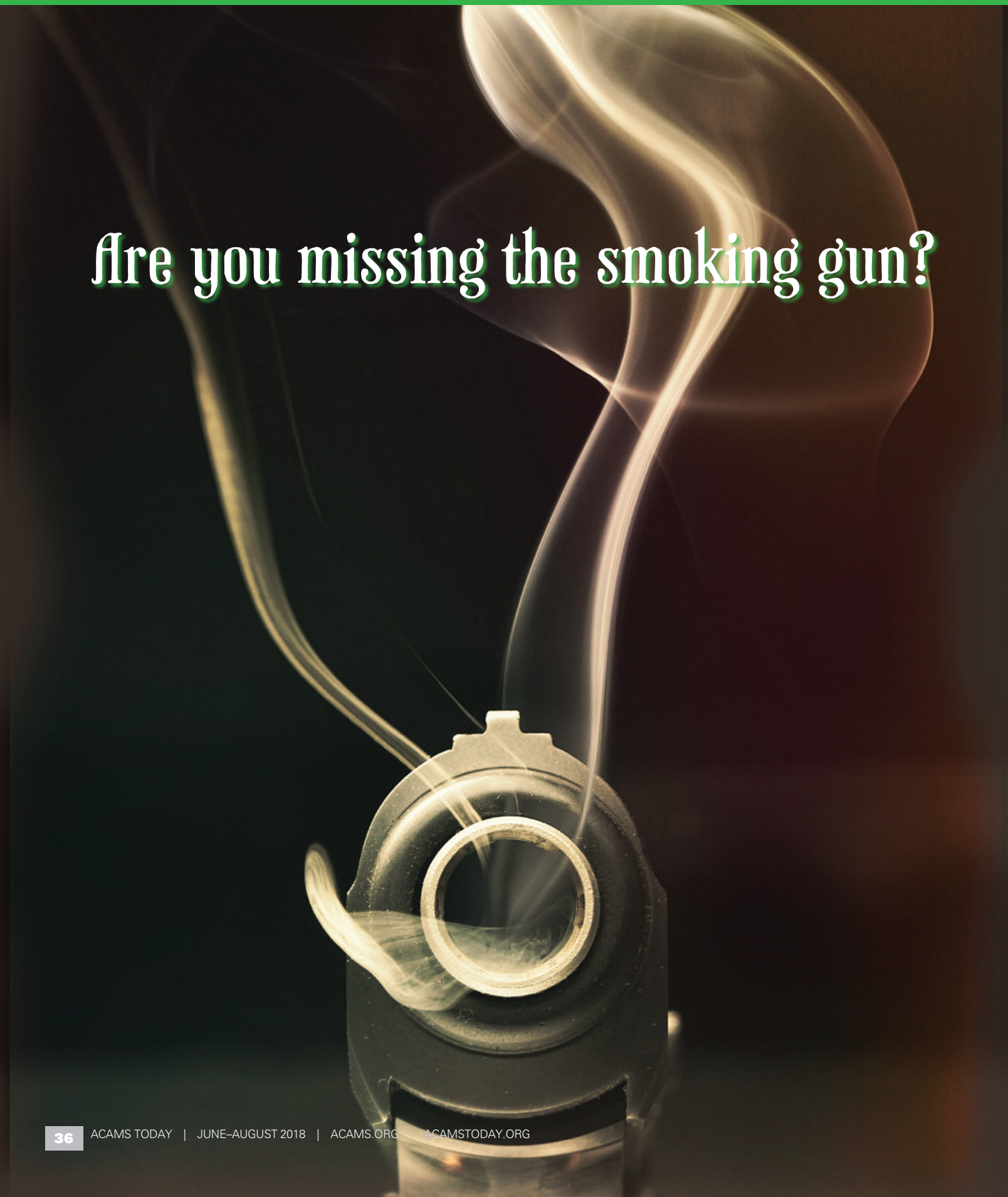
The independent testing requirement of the BSA is not easy but when it is done well, it can help gauge the status of your compliance program. Being proactive to ensure the reviewers have the appropriate contextual information and the test meets regulatory minimums is a sound strategy for success.

Elaine Yancey, CAMS, managing examiner, Federal Reserve Bank of Richmond, Richmond, VA, USA, elaine.yancey@rich.frb.org

The views and opinions expressed here are those of the author and do not represent an official position of the Federal Reserve Bank of Richmond or the Federal Reserve System.

[1] "Bank Secrecy Act/Anti-Money Laundering Examination Manual," Federal Financial Institutions Examination Council, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm

Are you missing the smoking gun?



As techniques, typologies, schemes and conduits used for money laundering and terrorist financing become more complex, sophisticated and less transparent, the ability to prove an individual(s) is criminally culpable will continue to be a challenge faced by attorneys, law enforcement and criminal investigators throughout the industry. Parallel that challenge with the fact that financial institutions may inadvertently not be providing all of the transactions related to the individual as part of a subpoena request, in-turn further aggravating the ability to truly follow the money. The solution to intersecting these two challenges while enhancing the effectiveness of an investigation is understanding the issue with current subpoena language typically used in a financial-related investigation(s); understanding the need to evolve the subpoena language; and recognizing how the work performed within the anti-money laundering/Bank Secrecy Act (BSA/AML) department of a financial institution may serve as a form of intelligence to your investigation. Evolving the thought, approach and application of the recommendations herein may serve as a catalyst to transform the success of financial investigations and the quality and accuracy of financial information obtained through a subpoena.

The issue and possibly your smoking gun

When a financial institution receives a subpoena, the standard wording may request a customer's account activity via statements, loan documents or transaction activity for a certain period. In response to the subpoena and what appears to be the norm, a financial institution will provide statements as the customer's record of activity. However, by providing or just reviewing the statements, there could be hidden transactions of which financial institutions may not be aware. Typically, these transactions may include, but are not limited, to cash advances, currency exchanges (foreign and domestic), foreign exchange wires and cashed items (on-third-party checks and us). In addition, monetary instrument purchases are also susceptible to not showing on the statement, but not as often as the previously listed transactions.

The example to the right demonstrates where financial institutions may be missing part of the money flow; especially, if they are relying on the customer statement to identify all monetary transactions linked to potentially illicit activity. The first image is a basic monthly statement provided by most financial institutions and what would be assumed to serve as the document to follow the money during an investigation. The same activity within the second statement contains all the "hidden" information and transactions that are not often reflected in a statement and therefore typically not provided as part of a subpoena request, though they should be.

Typical Statement

DEPOSITS

10-Jul	Counter Deposit	$8,000
15-Jul	ACH Deposit – ABC Company Payroll	$1,908.44
16-Jul	Counter Deposit	$1,200
20-Jul	ATM Deposit	$4,200
28-Jul	Counter Deposit	$4,500
30-Jul	ACH Deposit – ABC Company Payroll	

WITHDRAWALS

3-Jul	ATM W/D – Main Street	$500
03-Jul	POS Debit – Main St. Grocery	$176.02
11-Jul	Branch Withdrawal	$5,000
15-Jul	Misc. Withdrawal – Main Street Branch	$7,000
21-Jul	POS Debit – Auto Fixers	$204.87
22-Jul	Check #1334	$764.99
28-Jul	Outgoing Wire	$15,500

Statement with (Hidden) Activity

DEPOSITS

10-Jul	Counter Deposit ($10,000 check with $9,000 back in cash)	$1,000
10-Jul	Counter Deposit (cash)	$7,000
15-Jul	ACH Deposit – ABC Company Payroll	$1,908.44
16-Jul	Counter Deposit (cash)	$1,200
20-Jul	ATM Deposit ($1,200 check; $3,000 cash)	$4,200
20-Jul	Counter Deposit (cash)	$5,000
30-Jul	ACH Deposit – ABC Company Payroll	$1,908.44

WITHDRAWALS

03-Jul	ATM W/D – Main Street	$500
03-Jul	POS Debit – Main St. Grocery	$176.02
05-Jul	Foreign Currency Order (customer requested order of Euros)	$3,000
11-Jul	Counter Withdrawal (cash)	$5,000
15-Jul	Misc. Withdrawal – Main Street Branch (FX wire to China via Big Bank USA)	$7,000
16-Jul	Cash Advance (customer used a credit card not issued by this bank)	$6,000
21-Jul	POS Debit – Auto Fixers	$204.87
22-Jul	Check #1334	$764.99
24-Jul	Bank Withdrawal (cashier check purchase with $2,800 in cash; $7,000 W/D from account)	$9,800
24-Jul	Check Cashed (on-us from another bank customer)	$5,000
28-Jul	Outgoing Wire (wire to Guernsey via BankersBankUSA)	$15,500
31-Jul	Currency Exchange (U.S. dollars for U.S. dollars)	$3,900

Seize the value

There are several critical reasons why obtaining the hidden information is important to an investigation. Not only does it allow for following the money and uncovering all potential illicit proceeds involved in the suspected crime, it can directly impact whether or not a case is "worth" prosecuting.

For instance, two different banks in the same town received subpoenas regarding a single business customer. The projected total dollar amount of funds related to the suspected underlying activity was estimated to be $1,250,000. The banks provided the standard information requested in subpoenas that included bank statements, check copies and account-opening documentation. However, the total dollar amount after the subpoena responses were received only totaled $810,000. The interest in prosecuting this case waned given the lower dollar amount. One of the banks subpoenaed filed a suspicious activity report (SAR) for the activity. Federal law enforcement agents requested the SAR backup documentation in an attempt to reconcile the difference in the total dollar amounts. Nevertheless, the backup documentation was similar to the subpoenaed documentation. The senior agent spoke to the BSA officer and explained the issues they were seeing in the transactions listed in the narrative and how they were not showing in the statement. The BSA officer pulled several ad-hoc reports from the anti-money laundering (AML) system that showed $580,000 of transactions (just for this one bank) that had not been passed through to the statement. The BSA officer amended the SAR filing to include the specific backup documentation showing the "hidden" transactions. The agency issued a new subpoena with clearer language that resulted in the bank providing ad-hoc reports evidencing the additional $580,000 of transactions. These results from the bank were mirrored when a new subpoena was issued for the other bank involved. The other bank was able to provide, through ad-hoc reporting, an additional $1,115,000 of transactions. In total, the amount of suspected activity and documentation obtained through the revised subpoena increased from $810,000 to $1,695,000.

Evolution of subpoena language

To ensure all applicable customer transactions are received as part of a subpoena request, law enforcement must understand how various transactions can be performed at the teller line or in the wire department. Not all financial transactions are reflected or linked to a customer's account. This additional transaction information may lie within other internal financial systems, such as teller platforms, general ledgers, wire systems, third-party software and AML monitoring systems. In smaller community banks and credit unions, this information may further reside on manual excel spreadsheets or even on paper logs in the branches.

> Not all financial transactions are reflected or linked to a customer's account

Second, consideration to the standard subpoena language should evolve to include the recommended verbiage below, or at least a version of it. This will assist in obtaining all the information needed, including what may be the smoking gun embedded in these "hidden" transactions and transparency to all proceeds involved in the suspected criminal activity. In addition, this language serves to steer the receiver of the subpoenas, which is typically the operations or research department of a financial institution, to contact the BSA/AML department to fulfill the specific subpoena requests. This is a vital step as most institutions are unaware that they are not providing the full transaction profile of the customer when responding to subpoena requests.

The standard subpoena language will ordinarily state verbiage similar to, "Provide any and all documents pertaining to all open or closed checking, savings, negotiable order withdrawal (NOW), time, or other deposit or checking accounts for the named parties or entities, including bank statements."

This standard language is surface level and will likely result in missed transactions. Recommended verbiage to include within a subpoena can be found below. The evolution of this language should assist in obtaining all the valuable information needed to conduct an investigation.

> "In compliance with this subpoena request, please provide all transactional activity, including but not limited to transactions recorded outside the core system. This activity should include the following:
>
> - Cash activity, including deposits and withdrawals;
> - Cash advances;
> - Credit and debit memos;
> - Deposit slips, items deposited;
> - Currency exchanges (foreign and domestic);
> - Cashed third-party and cashed on-us checks;
> - Wires originated online and in branch;
> - Foreign, domestic and foreign exchange (FX) wires;
> - Monetary instrument purchases or encashments performed by or on behalf of the customer;
> - Checks negotiated against the customer's account and all check deposits;
> - Account transfers including the receiving/sending account numbers;
> - Payment 2 Payment (P2P) details;
> - Automated Clearing House (ACH) debits and credits, including International ACH transactions (IAT).

> Transaction activity reports maintained outside the core system and monthly statements can contain valuable information. The requested transactions may reside in auxiliary systems and could include anti-money laundering systems, wire systems, cash advance systems, and foreign currency order or exchange systems."

In addition to the language above, consider requesting, as applicable, any and all enhanced due diligence (EDD) and high-risk customer (HRC) reviews conducted during the time frame, account-opening documents, including any customer due diligence (CDD)/account opening questionnaires, beneficial owner information and a beneficial ownership certification form(s). Secondly, consider requesting any alert, case reviews or similar analysis such as internal investigation performed on the customer through the financial institution's suspicious activity monitoring or fraud software; however, ensure verbiage includes the omission of any information or documentation that indicates the existence of a SAR filing. Requests for alerts within the bank's automated transaction monitoring system could state, "Any alerts generated through the bank's transaction monitoring processes (e.g., the bank's AML department/software) that included accounts or transactions pertaining to the named parties, regardless if the alert resulted in a regulatory filing. For any alerts and/or cases, please provide the parameters that were triggered."

As a supplement to the recommended verbiage, including an example illustration similar to the earlier example may assist financial institutions in understanding why additional information—outside of the statement—is requested.

Bank investigative intelligence

While transaction activity reports maintained outside the core system and monthly statements can contain valuable information for an investigator, there is an additional treasure trove of information and data—or intelligence—that most financial institutions possess. In-depth documented reviews, consisting of analyzing data based off collected information have likely been performed on a customer(s) to comply with regulations such as the BSA and USA PATRIOT Act (USAPA) throughout the relationship.

At customer account opening and periodically throughout the relationship, financial institutions gather additional information outside of the identifying information required under the USAPA and a signature card. Through CDD, additional information may be obtained including the nature and purpose of the account, anticipated activity, high-risk indicators such as whether the individual is a politically exposed person, money services business, private ATM owner, or involved in the cultivation or distribution of marijuana. This information is typically documented and retained on account-opening questionnaires or customer onboarding systems. Furthermore, on May 11, 2018, financial institutions began identifying and verifying the identity of beneficial owners and controllers of all legal entities (other than those excluded) customers. This information is documented and certified by the individual opening the account and can be provided to law enforcement, investigators or attorneys with key details about suspected criminals who may use legal structures to conceal their illicit activities and/or assets.

In addition, financial institutions perform and document ongoing full-scale reviews on HRCs which typically include a six-to-12 month transactional analysis; results of third-party searches, extensive external research through publicly available open-source information; explanations of the nature of the business or source of income including revenue analysis; big data linkage of relationships or transactions with other customers or businesses; and a review of necessary federal, state or county licenses and registrations. This information—characteristically referred to as HRC reviews or EDD reviews—could potentially provide critical information in a clear and concise manner resulting in a form of intelligence for law enforcement and a storybook for an attorney.

There is an additional treasure trove of information and data —or intelligence— that most financial institutions possess

Two possible reasons this information is not typically included are it might not be directly referenced in the subpoena or the department or individuals responsible for addressing the subpoena are not aware this information exists. Requesting this information specifically in a subpoena request gently guides the subpoena receivers to the BSA/AML department. This will increase the opportunity to receive the valuable information needed.

Conclusion

Sherlock Holmes said, "It has long been an axiom of mine that the little things are infinitely the most important." While financial institutions are responding to subpoenas in good faith, the hidden transactions not seen on an account statement may one day be the smoking gun law enforcement has been tirelessly searching for and can materially increase the dollar amount of the investigation. Furthermore, leveraging the depth of diligence and reviews that may have been performed on one's subject throughout their relationship with the financial institution may serve as conduit to further understand the subject, linked relationships, transaction and data insight, associated accounts, and disparate pieces of information that will theoretically serve as a form of intelligence to an investigation. By transforming the thought and approach of subpoena language, a road map to receiving valuable and accurate financial information from the financial institution will emerge, resulting in more effective and efficient financial investigations.

Sarah Beth Felix (Whetzel), CAMS, MFS, president, Palmera Banking Solutions, Austin, TX, USA, sarah@palmeraconsulting.com

Lauren Kohr, CAMS-FCI, SVP, chief risk officer, Old Dominion National Bank, Tysons Corner, Virginia, USA, LKohr@ODNBonline.com

Subpoena Avenue

CYBERSECURITY:
CONFRONTING IMPERSONATION FRAUD AS BANKS REORGANIZE

High-profile organizational changes in banks and other financial institutions may present media-savvy fraudsters with opportunities to commit scams on unsuspecting customers. Law enforcement, financial institutions and the government should continuously recalibrate how they partner to address fraud, which could be far too complex for each to manage alone.

A timely case in point is the reorganization of larger banks in the U.K. in response to the Financial Services (Banking Reform) Act 2013[1] (the Banking Reform Act), which demonstrates the need to think ahead of fraudsters, money launderers and cybercriminals to protect financial institutions and their employees and customers.

Regulatory context

The Banking Reform Act imposes higher standards of conduct on U.K. banks and bolsters their loss-absorbing capacity to avoid taxpayer bailouts. Key provisions require larger U.K. banks to segregate their own retail and investment banking to protect the U.K.'s banking and financial systems.[2]

To comply with such "ring-fencing" regulations, larger U.K. banks must separate their own banking services for individuals and businesses (like checking and savings accounts assigned to the "ring-fenced bank") from risks in other parts of their business (like investment banking assigned to the "non-ring-fenced bank").[3]

Ring-fenced and non-ring-fenced bank subsidiaries must be independent operationally and organizationally, although each

[1] "Financial Services (Banking Reform) Act 2013 c.33," legislation.gov.uk, http://www.legislation.gov.uk/ukpga/2013/33/contents

[2] Timothy Edmonds, "Banking Services: Reform and Issues"¨ Briefing Paper Number 07234, *House of Commons Library*, December 22, 2017, researchbriefings.files.parliament.uk/documents/CBP-7234/CBP-7234.pdf

[3] "Ring-Fencing and Halifax," Halifax, https://www.halifax.co.uk/helpcentre/ring-fencing-and-halifax/

may operate alongside the other. By January 1, 2019, new sort codes and customer account numbers must be reassigned. Ring-fencing may affect about 75 percent of U.K. consumer banking deposits.[4]

Banking Reform Act ring-fencing has been influenced by the Depression era's Glass-Steagall Act of 1933, when each U.S. bank was given one year to choose whether to remain in either commercial banking or investment banking.[5] The Glass-Steagall model was followed in 1948, when post-World War II Japan adopted a legal separation of commercial banking and investment banking.[6] Glass-Steagall was repealed in 1999. Yet, the topic of a loosely defined "21st Century Glass-Steagall" in the U.S. has recently enjoyed diverse political support ranging from the far left to the far right.[7]

U.K. banks affected

The Banking Reform Act applies to the U.K.'s largest banks with more than 25 billion pounds (averaged over a three-year period) in consumer and small business deposits.[8] Specifically:

- Barclays
- HSBC
- Lloyds Banking Group, including Lloyds Bank, Bank of Scotland and Halifax brands
- Royal Bank of Scotland (RBS) Group, including Adam & Company and National Westminster Bank (NatWest) brands
- Santander

RING-FENCING MAY AFFECT ABOUT 75 PERCENT OF U.K. CONSUMER BANKING DEPOSITS

Potential service "disruption"

In a June 16, 2017 speech to the British Bankers' Association, James Proudman, the executive director for the U.K. Deposit Takers Supervision at the Bank of England, foreshadowed possible U.K. bank "disruption" due to Banking Reform Act compliance.[9]

Yet, eight months after this speech, a Google U.K. search of the words "ring-fencing bank disruption" does not readily display one prominent website that centralizes practical details on such U.K. bank "disruption," presenting media-savvy fraudsters with opportunities to exploit uneven public information from Barclays, HSBC, Lloyds Bank, RBS Group and Santander.

Barclays notified its online, phone and mobile banking customers proactively that they would experience web blackouts one weekend per month between August 2017 and January 2018.[10] *ComputerWeekly*[11] reported that planned blackouts should result in Barclays being compliant with the Banking Reform Act in April 2018[12]—about eight months ahead of the January 1, 2019 deadline.

Regarding HSBC, *The Telegraph* used the term "disruption" in a report about service delays that could occur as account numbers and sort codes are changed for 170,000 customers, payments are redirected and cards are replaced.[13]

Social engineering alerts

Affected U.K. banks have reminded their employees and customers proactively to watch out for fraudsters, who could use impersonation fraud, also called social engineering, to obtain sensitive information (such as usernames, passwords, account numbers and credit card numbers) through:

- Emails, pop-up windows and websites (called "phishing")
- Telephone calls, caller ID spoofing and voicemail (called "vishing," a combination of "voice" and "phishing")

[4] James Proudman, "Putting Up a Fence," Bank of England, June 16, 2017, https://www.bankofengland.co.uk/speech/2017/putting-up-a-fence

[5] Julia Maues, "Banking Act of 1933 (Glass-Steagall)," Federal Reserve History, November 22, 2013, https://www.federalreservehistory.org/essays/glass_steagall_act

[6] Michelle Clark Neely, "Commercial & Investment Banking: Should This Divorce Be Saved?," Federal Reserve Bank of St. Louis, April 1995, https://www.stlouisfed.org/publications/regional-economist/april-1995/commercial--investment-banking-should-this-divorce-be-saved

[7] Matt Egan, "Trump Wants to Revive a 1933 Banking Law. What That Means is Very Unclear," *CNN Money*, May 9, 2017, http://money.cnn.com/2017/05/09/investing/donald-trump-glass-steagall/index.html

[8] "Ring-Fencing," UK Finance, https://www.ukfinance.org.uk/ring-fencing/

[9] Huw Jones, "BoE Warns of Potential Disruption from Ring-Fencing Banks," *Reuters*, June 16, 2017, https://uk.reuters.com/article/uk-boe-banks-ringfencing/boe-warns-of-potential-disruption-from-ring-fencing-banks-idUKKBN1971BF

[10] Chris Lemmon, "Barclays Warns of 'Web Blackouts' Until 2018," *FStech*, August 17, 2017, http://www.fstech.co.uk/fst/Barclays_Web_Blackouts_Warning.php

[11] Karl Flinders, "Barclays Bank Ahead of Schedule in Ring-Fencing Project," *ComputerWeekly.com*, September 7, 2017, http://www.computerweekly.com/news/450425918/Barclays-Bank-ahead-of-schedule-in-ring-fencing-project

[12] "Preparing for Ring-Fencing," Barclays, https://www.home.barclays/about-barclays/ring-fencing-explained.html

[13] Sam Meadows, "HSBC Changes 170,000 Customers' Sort Codes: What You Need to Know," *The Telegraph*, August 2, 2017, http://www.telegraph.co.uk/personal-banking/current-accounts/hsbc-change-170000-customers-sort-codes-need-know/

- Text messages (called "smishing," a combination of "SMS" and "phishing").[14]

The Barclays website even offers a phone number checker, so that customers might verify whether a bank phone number is genuine.[15]

Volume of changes and related publicity

The reported volume of changes varies widely among the U.K.´s largest banks.[16] About 900,000 Barclays accounts moved to new six-digit sort codes.[17] A smaller number of HSBC and RBS customers were affected. About 10,000 Santander customers moved to new sort codes. Few Lloyds customers were affected.[18]

Such reported details could encourage fraudsters to target customers of certain larger U.K. banks, based on the volume of sort code or account changes. Larger U.K. banks have information online to warn customers of fraud threats, which, in turn, warns fraudsters that they are being watched.

Still, larger U.K. banks have public webpages on ring-fencing with open-ended statements, like, "If your business is going to be affected by these changes, we will contact you to let you know what this means for you."[19]

A fraudster could interpret such an open-ended statement as a cue to impersonate a bank employee and reach out to unsuspecting customers by letter, email, call or text message.

IMPERSONATION FRAUD LOSSES CAN BE SUBSTANTIAL

Impersonation fraud

U.K. banks may also communicate with customers through password-protected online banking. However, fraudsters reportedly obtain U.K. bank accounts by impersonating existing bank customers.[20] Money launderers reportedly buy U.K. bank accounts from foreign students (who then become "money mules") before they leave the U.K.[21]

Impersonation fraud challenges U.K. banks that allow customers to open accounts online.[22] Bank employees have helped fraudsters to impersonate customers of large U.K. bank accounts, so that money might be stolen, laundered through sham companies and then moved offshore.[23]

Lloyds reports that the most common impersonation fraud types are CEO fraud (fraudulent payment instructions from corporate decision-makers) and invoice fraud (fraudulent payment instructions from a supplier or vendor).[24]

Coverage for losses

Impersonation fraud losses can be substantial. Yet, insurers may not classify theft from impersonation fraud as a cyberattack (if data was not stolen) or as a crime loss (if an employee unknowingly but voluntarily furthered the fraud).[25]

[14] "Recognize Fraudulent Emails and Websites," PayPal, https://www.paypal.com/us/webapps/mpp/security/suspicious-activity

[15] "Protect Yourself from Fraudsters," Barclays, https://www.barclays.co.uk/security/

[16] Caroline Binham and Emma Dunkley, "Regulators Get Ready to Authorise 'Ringfenced' UK Banks," *Financial Times*, August 18, 2017, https://www.ft.com/content/5ca81a48-8372-11e7-a4ce-15b2513cb3ff

[17] Jill Treanor, "Banks Issue New Sort Codes in Ringfencing of High Street Operations," *The Guardian*, August 6, 2017, https://www.theguardian.com/business/2017/aug/06/banks-reissue-sort-codes-in-ringfencing-of-high-street-operations

[18] Adam Williams, "Bank Customers Set for Sort Code and Account Number Switch—Are you affected?," *Moneywise*, July 5, 2017, https://www.moneywise.co.uk/news/2017-06-29/bank-customers-set-sort-code-and-account-number-switch-—are-you-affected

[19] "What Ring-Fencing Means for our Business Banking and Commercial Clients," Lloyds Banking Group, http://www.lloydsbankinggroup.com/our-group/ring-fencing/business-banking-and-commercial-clients/

[20] "Cybercrime: Overseas Students Selling Bank Accounts to Fraudsters after Finishing Studies, Police," *iNews*, July 21, 2017, https://inews.co.uk/news/uk/cyber-crime-overseas-students-selling-bank-accounts-fraudsters-finishing-studies-police/

[21] "Overseas Students Targeted by Bank Account Fraudsters," *BBC News*, September 16, 2016, http://www.bbc.com/news/av/uk-england-london-37339023/overseas-students-targeted-by-bank-account-fraudsters

[22] Faye Lipson, "ID Theft: How Bank Account Fraudsters May Steal Your Identity," *Which?*, September 23, 2017, https://www.which.co.uk/news/2017/09/id-theft-how-bank-account-fraudsters-may-steal-your-identity/

[23] Russell Myers, "Bank Workers Jailed for Part in Huge Fraud that Netted Millions from Right Lloyds TSB Customers," *Mirror*, July 24, 2017, https://www.mirror.co.uk/news/uk-news/bank-workers-jailed-part-huge-10864216

[24] "How to Help Protect Your Business Against Impersonation Fraud," Lloyds Bank, July 10, 2017, http://resources.lloydsbank.com/insight/gameplan/how-to-help-protect-your-business-against-impersonation-fraud/

[25] "Social Engineering/Impersonation Fraud," Marsh & McLennan Agency, September 8, 2015, http://www.marshmma.com/Blog/SocialEngineeringImpersonationFraud.aspx

RAISING PUBLIC AWARENESS ABOUT SOCIAL ENGINEERING, FRAUD AND EXPLOITATION IS CRITICAL FOR CERTAIN CUSTOMERS WHO MAY BE SUSCEPTIBLE TO SCAMS

Social engineering fraud insurance is growing in popularity as a viable alternative. For coverage, insured customers should have processes to protect themselves from social engineering.[26]

Targeting scam alerts

Raising public awareness about social engineering, fraud and exploitation is critical for certain customers who may be susceptible to scams,[27] including elderly[28] and vulnerable[29] customers, new immigrants and individuals who are not fluent in English.[30]

Fraudsters could exploit the elderly concerned about pension funds being sponsored by non-ring-fenced banks, which have been portrayed as more volatile than ring-fenced banks.[31] At HSBC and Santander, pension funds are being sponsored by ring-fenced banks and at Barclays, they are being sponsored by a non-ring-fenced bank.[32]

Yet, Barclays' research in the U.K. indicates that stereotypes about older customers being more vulnerable do not apply to digital crimes.[33] A 2017 survey states that U.K. millennials between ages 25 to 34 experience more cybercrime than older respondents, who scored higher on digital safety awareness than younger respondents. U.K. millennials are twice as likely to be victimized by online fraud as are older respondents.[34]

Forbes recently reported similar survey results in the U.S., where millennials are more likely to be victims of digital crimes. U.S. millennials are more accustomed to using social media share buttons to give out personal information. They are more likely to believe that technology will shield intrusions, and that communications service providers bear responsibility for

[26] "The Hustle," *Chubb Progress*, 2017 Issue 2, 2017, https://www2.chubb.com/uk-en/_assets/documents/progress-issue-2-2017.pdf

[27] Dav Laura Shannon, "Banks Ring-Fencing Could Trigger a Spate of Scams," This is Money, January 6, 2018, http://www.thisismoney.co.uk/money/saving/article-5241771/Banks-ring-fencing-trigger-spate-scams.html

[28] Sid Kirchheimer, "Caller ID Scams on the Rise—Fraudulent Calls Threaten Your Money and Your Identity," *AARP Bulletin*, https://www.aarp.org/money/scams-fraud/info-05-2012/caller-id-scams-on-rise.html

[29] Mark Byers, "Proposed Barclays Ring-Fencing Transfer Scheme—Report of the Skilled Person under Section 109A of the Financial Services and Markets Act 2000," Grant Thornton UK LLP, October 23, 2017, https://www.home.barclays/content/dam/barclayspublic/docs/AboutUs/ringfencing/REPORT%20-%20Barclays%20Ring-Fencing%20Transfer%20Scheme.pdf

[30] "Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation," BITS, November 2, 2012, https://www.acl.gov/sites/default/files/programs/2016-09/Smocer_White_Paper.pdf

[31] Patrick Jenkins, "Why UK Bank Ringfences Don't Make Everyone Safer," *Financial Times*, December 18, 2017, https://www.ft.com/content/1d529c3c-e1a6-11e7-a8a4-0a1e63a52f9c

[32] Susanna Rust, "HSBC, Santander Reveal Ring-Fencing Plans for Pension Schemes," *IPE*, January 25, 2018, https://www.ipe.com/news/pensions/hsbc-santander-reveal-ring-fencing-plans-for-pension-schemes/10022844.article

[33] "Barclays Digital Safety Index 2017: Summary of Key Findings," Barclays, https://www.home.barclays/content/dam/barclayspublic/docs/BarclaysNews/2017/May/Barclays%20digital%20safety%20exec.%20summary.pdf

[34] "The Great British Fraud Fightback," Barclays, May 8, 2017, https://www.home.barclays/news/2017/05/the-great-british-fraud-fightback.html

filtering out fraudulent email, calls and text messages from reaching their computers and mobile devices.[35]

Banks on high alert for cyberattacks

Ring-fencing compliance includes U.K. ring-fenced and non-ring-fenced banks separating their IT systems, operations and agreements with suppliers, licensors and vendors.[36] U.K. banks have been cautioned to train staff proactively, treat all bank communications with care, and encrypt transferred data[37] consistent with the U.K.'s Data Protection Bill and the EU's General Data Protection Regulation (GDPR).[38]

There have been news reports of U.K. bank employee changes, presenting media-savvy fraudsters with opportunities to exploit employee confusion.[39]

In early 2017, *Reuters* reported on Barclays' plans to overhaul back-office operations, affecting more than 10,000 people who support back-office operations in 17 countries. HSBC had to transfer 18,000 people who support back-office operations to a U.K.-based service company in 2015, with plans to shift an additional 1,000 persons from London to Birmingham.[40]

Barclays became the first major U.K. bank to obtain final approval for its ring-fencing transfer scheme in early March 2018, when the presiding High Court judge considered and dismissed pensions agreement concerns.[41]

Key takeaways

- When planning a reorganization at a bank or other financial institution, include information security early in the planning process, along with other key internal stakeholders such as public relations, fraud, data protection, government affairs, customer service and marketing
- Diversify identity verification beyond know your customer (KYC) checks to include other elements, such as two-factor authentication, confirmation email, internet protocol (IP) addresses, geolocation data, device identifiers like media access control (MAC) addresses, operating system and browser attributes, application data, website activity and app usage data[42]
- If other banks or financial institutions are reorganizing due to regulations, consider collaborating with them on one prominent website that provides practical public updates and links to affected entities, especially if service disruptions are expected
- Before any information is made public, consider how media-savvy fraudsters might use it to detect opportunities to exploit organizational changes[43] and target vulnerable individuals[44]
- Check cybersecurity practices of public relations consultants and newswire services to avoid fraudsters being tipped off to press releases[45]
- Partner with law enforcement to deter fraud by educating the public on fraud, money laundering and cybercrimes, as Barclays, RBS, Financial Fraud Action UK and the Metropolitan Police Service of London did with the publication of *The Little Book of Big Scams*[46]

PARTNER WITH LAW ENFORCEMENT TO DETER FRAUD BY EDUCATING THE PUBLIC ON FRAUD, MONEY LAUNDERING AND CYBERCRIMES

[35] Kelly Phillips Erb, "Millennials Most Likely To Fall Victim To Tax and Financial Scams," *Forbes*, June 25, 2017, https://www.forbes.com/sites/kellyphillipserb/2017/06/25/millennials-most-likely-to-fall-victim-to-tax-financial-scams/#3add114d5353

[36] Karl Flinders, "Barclays ring-fencing project means downtime for customers," Karl Flinders, *ComputerWeekly.com*, August 17, 2017, http://www.computerweekly.com/news/450424615/Barclays-ring-fencing-project-means-downtime-for-customers

[37] Stefania Spezzati and Suzi Ring, "Cyber Threat Looms for U.K. Banks as Ring-Fencing Exposes Data," *Bloomberg*, November 15, 2017, https://www.bloomberg.com/news/articles/2017-11-16/cyber-threat-looms-for-u-k-banks-as-ring-fencing-exposes-data

[38] "Data Protection Bill [HL]," U.K. Parliament, January 18, 2018, https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/en/18153-EN.pdf

[39] Israel Levy, "The insider threat: the biggest threat in banking cyber-security," *SC Media UK*, May 19, 2017, https://www.scmagazineuk.com/the-insider-threat-the-biggest-threat-in-banking-cyber-security/article/654525/

[40] Lawrence White, "Barclays to overhaul back office operations to cope with ring-fencing," *Reuters*, February 5, 2017, https://uk.reuters.com/article/uk-barclays-restructuring/barclays-to-overhaul-back-office-operations-to-cope-with-ring-fencing-idUKKBN15K0AT

[41] Stephanie Baxter, "High Court Judgment Dismisses Pension Concerns Over Barclays Ring-Fencing Transfer," *Professional Pensions*, March 12, 2018, https://www.professionalpensions.com/professional-pensions/analysis/3028216/high-court-judgment-dismisses-pension-concerns-over-barclays-ring-fencing-transfer

[42] Will Wyatt, "Why Know Your Customer (KYC) Isn't Fraud Prevention," *Whitepages Pro*, September 25, 2017, https://pro.whitepages.com/blog/know-customer-isnt-fraud-prevention/

[43] "UK Bank Ring-Fencing a Fraudster's Charter," *Treasury Today*, September 2017, http://treasurytoday.com/2017/09/uk-bank-ring-fencing-a-fraudsters-charter-ttti

[44] Steve Ragan, "Scammers Using Obituary Notices to Acquire New Victims," *CSO*, February 15, 2015, https://www.csoonline.com/article/2885141/malware-cybercrime/scammers-using-obituary-notices-to-acquire-new-victims.html

- Law enforcement, banks and government should partner to overhaul fraud reporting tools[47] and protocols[48] that are underperforming in the eyes of the public
- Review websites that present ways to protect personal customers,[49] business and corporate clients,[50] and business banking clients,[51] and options like social engineering fraud insurance
- Obtain periodic input from demographically diverse bank customers on fraud and cybersecurity issues, so that their input might be integrated into digital safety awareness planning and development
- To combat financial fraud, banks and financial institutions should be encouraged to share fraud data internally and with competitors and law enforcement,[52] as USA PATRIOT Act sections 314(a) and 314(b) are used to enhance anti-money laundering/counter-terrorist financing compliance.[53]

Sooner or later, lawmakers in countries like the U.S. will raise the issue of separating commercial banking from investment banking, especially if U.K. bank ring-fencing is executed successfully by January 1, 2019. A "21st Century Glass-Steagall" version influenced by U.K. bank ring-fencing should prompt law enforcement, banks and the government to think ahead of media-savvy fraudsters, money launderers and cybercriminals, who could exploit new bank sort codes and reassigned customer account numbers.

Miguel Alcántar, CAMS-FCI, compliance advisor, Oakland, CA, USA, alcantar@aya.yale.edu

[45] Lily Hay Newman, "Press Releases Finally Get a Devoted Readership: Hackers," *Wired*, August 10, 2016, https://www.wired.com/2016/08/press-releases-finally-get-devoted-readership-hackers/

[46] "The Little Book of Big Scams," Metropolitan Police Service, 2015, https://www.met.police.uk/globalassets/downloads/fraud/the-little-book-of-big-scams.pdf

[47] Victoria Bischoff, "Dial 555 for Bank Fraud," *Daily Mail Online*, October 18, 2017, http://www.dailymail.co.uk/news/article-4994764/Police-plan-new-hotline-modelled-999-emergency-number.html

[48] Nathan Kay, "UK's New 'Banking Protocol' Stops £9 Million of Fraud," *Finder UK*, December 13, 2017, https://www.finder.com/uk/uks-new-banking-protocol-stops-9-million-of-fraud

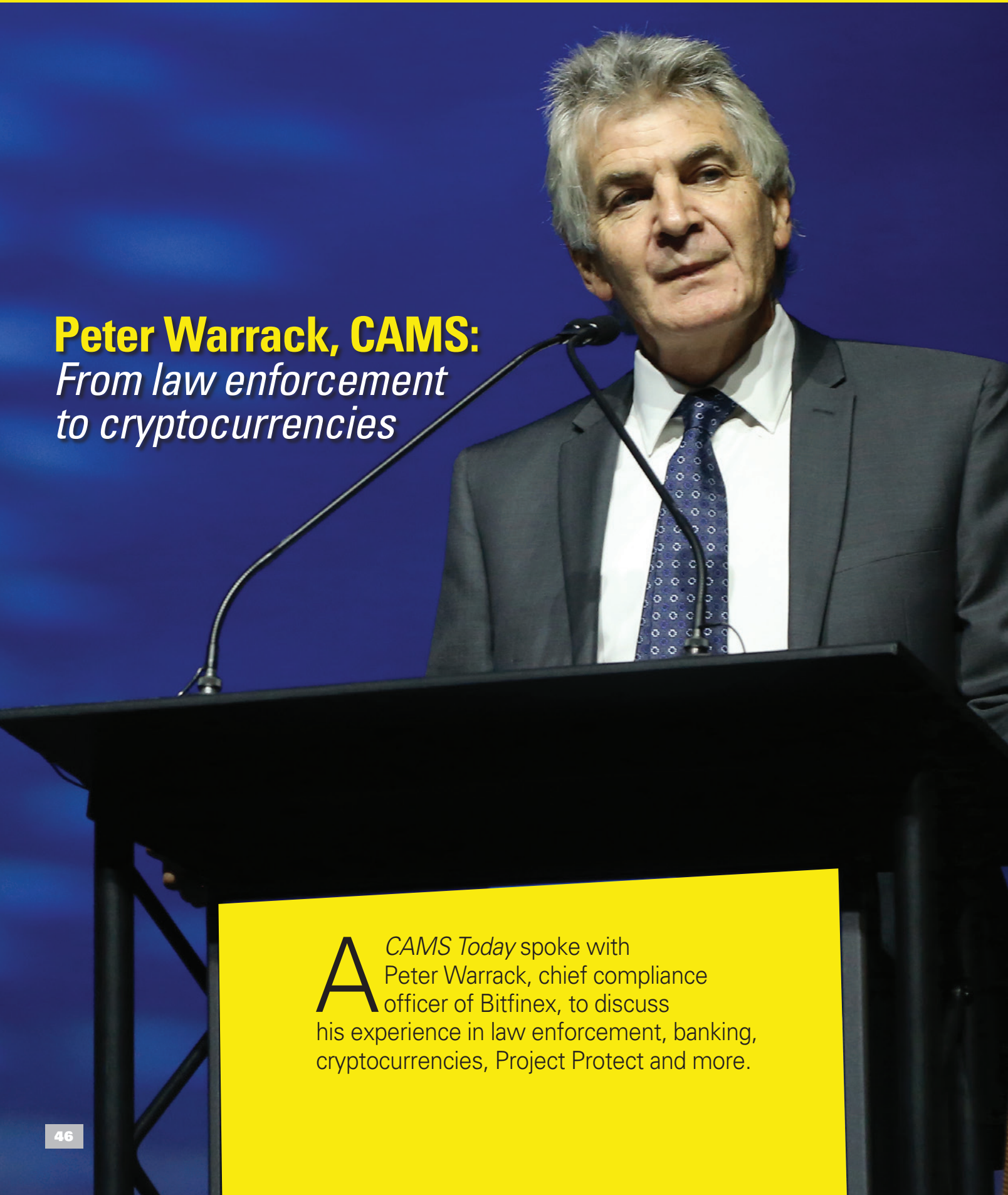
[49] "Protect Yourself from Fraudsters," Barclays, https://www.barclays.co.uk/security/

[50] "Fraud Smart Centre," Barclays, https://www.barclayscorporate.com/fraudawareness

[51] "Help Protect Your Business from Fraud," Barclays, https://www.barclays.co.uk/business-banking/manage/security/

[52] Stavros Gadinis and Colby Mangels, "Collaborative Gatekeepers," *Washington and Lee University School of Law Scholarly Commons*, 2016, https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4500&context=wlulr

[53] Penny Crosman, "How Data-Sharing Can Keep Fraud from Spreading," *American Banker*, March 24, 2014, https://www.americanbanker.com/news/how-data-sharing-can-keep-fraud-from-spreading



Peter Warrack, CAMS:
From law enforcement to cryptocurrencies

CAMS Today spoke with Peter Warrack, chief compliance officer of Bitfinex, to discuss his experience in law enforcement, banking, cryptocurrencies, Project Protect and more.

Peter Warrack, CAMS, CBP, CFE has over 15 years' experience in the Canadian and international banking sectors, specializing in intelligence-led major criminal, money laundering and terrorist financing investigations, anti-money laundering (AML) compliance, and the interaction between the traditional banking and virtual currency environments.

Prior to being headhunted by the Royal Bank of Canada (RBC) in 2002, Warrack had a successful career as a senior police officer and military intelligence officer based in the U.K.

Warrack's work was first recognized by ACAMS as the 2011 recipient of the *ACAMS AML Professional of the Year Award*, and again in 2017 as both the recipient of the *ACAMS AML Processional of the Year Award* and the *ACAMS Today Article of the Year Award* for his article, *When Two Worlds Collide*[1] which focused on the interactive banking and cryptocurrency environments.

In 2017, Warrack was also recognized by ACAMS for his work in addressing human trafficking and for his initiative Project Protect, a uniquely successful public-private sector partnership between the financial sector, law enforcement, Canada's financial intelligence unit, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), nongovernmental organizations and others. Its model has been recognized internationally by the U.N., the Organization for Economic Co-operation and Development, the Vatican Ethics in Action meeting on modern slavery, the Financial Action Task Force and the Egmont Group as best practice.

Warrack presents, teaches and publishes regularly on a range of subjects including major investigation management, AML, counterterrorist financing (CTF) investigations, virtual currencies for law enforcement and the application of blockchain technology.

I HAVE BEEN HIGHLIGHTING THE DEVELOPING RELATIONSHIP BETWEEN THE TRADITIONAL BANKING SECTOR AND THE VIRTUAL CURRENCY WORLD FOR SEVERAL YEARS NOW

ACAMS Today: You came to North America in 2002 from Northern Ireland, where you transitioned from law enforcement (LE) to banking. What led you to transition from LE to banking?

Peter Warrack: I had built up internationally recognized experience in investigating major crimes, and was also a proponent of an intelligence-led approach to crime, specifically preventing crime. This coincided with the RBC's strategy of a proactive approach to address crime and RBC made me an offer I couldn't refuse, which was to build and implement their intelligence program. It proved very successful.

I also brought with me, to the banking industry, experience in major investigation management, which RBC implemented as best practice; for example, coordinating the efforts of legal, fraud, corporate security, media relations and AML as major incidents arose.

AT: ***How did your background in LE help you build strong partnerships when you began working in the private sector?***

PW: My LE work entailed working on international investigations with LE around the world including Canada and the U.S. I was able to open the doors further between the private sector and LE, which quickly provided partnerships of mutual benefit in addressing crime, best practices in investigation and analytical techniques, and of course intelligence-sharing.

AT: ***You recently transitioned into the cryptocurrency industry. Congratulations on your new position as chief compliance officer at Bitfinex! Could you tell us how your background in LE and banking will help you in your new role?***

PW: Well firstly, I have been highlighting the developing relationship between the traditional banking sector and the virtual currency world for several years now. The *ACAMS Today* article, *When Two Worlds Collide,* is an example of this where I called out the interactive versus closed environments.[2] The *ACAMS Today* article, *The Blocktrain Has Left the Station* by Leonardo Real and Joseph Mari, also talks to this and the need, as AML professionals, to embrace the new skill sets that are and will be required in this emerging space.[3]

To answer the question, the experience I have gained in LE has equipped me with a real world understanding of criminals' modus operandi, and my experience in banking has allowed me to apply and share my experience in shaping investigators' knowledge and in advising on the design of transaction monitoring systems to detect money laundering, terrorist financing and sanctions transactions. My experience has also allowed me to develop meaningful relations with regulators who have witnessed the significant increase in suspicious transaction report/suspicious activity report (STR/SAR) filing and the quality of these filings.

AT: ***What challenges do you anticipate financial crime prevention professionals will face when dealing with cryptocurrencies?***

[1] Joseph Mari, Peter Warrack, Leonardo Real, "When Two Worlds Collide," *ACAMS Today*, September 2016, https://www.acamstoday.org/when-two-worlds-collide/

[2] Ibid.

[3] Leonardo Real and Joseph Mari, "The Blocktrain Has Left the Station," *ACAMS Today*, June 2017, https://www.acamstoday.org/the-blocktrain-has-left-the-station/

PW: The immediate challenge is a lack of knowledge. Banks that say they don't deal with virtual currency are blind to the fact that they do; they just don't have the ability to recognize it. Like cash, virtual currency is not bad, but in some cases it can be exploited by bad actors. Understanding this space and being able to recognize and mitigate the risk is an opportunity, i.e., a speculative risk. AML professionals urgently need to receive training and also be equipped with investigative tools such as blockchain intelligence, chain analysis, elliptic to monitor, analyze and understand virtual currency-related transactions and interactions.

AT: ***What unique challenges do purveyors of cryptocurrency face in meeting regulatory compliance?***

PW: The first challenge is that there is no ubiquitous and agreed regulatory expectations to be met. In some jurisdictions, cryptocurrency is viewed as property, in others it is viewed as digital assets, a commodity or as a currency, as in Japan.

In my new role I will actively do my part to engage in dialogue with the various regulators to provide input into shaping regulations, and shared understanding of the risks, (and benefits) of this new world.

AT: ***During the ACAMS moneylaundering.com AML & Financial Crime Conference in April, compliance officers in a poll said that customer due diligence/sanctions monitoring/transaction monitoring concerns are their biggest concerns when dealing with virtual currencies. What advice can you offer financial institutions reluctant to transact with the sector?***

PW: The future is coming—again the blocktrain has left the station. Those institutions that invest in understanding the space, benefits and risks will have the competitive advantage in my opinion.

AT: ***What are some of the due diligence best practices financial institutions should employ when dealing with clients from the cryptocurrency sector?***

PW: Again, understand the space and the risks. Onboarding and associated customer due diligence and know your customer processes are similar, in fact the exchange space in many cases exceeds those of traditional financial institutions. I think the greater challenge for institutions is in monitoring virtual currency transactions, particularly those involving privacy coins.

AT: ***How can financial institutions distinguish between rogue virtual currency entities and legitimate companies that follow AML compliance rules?***

PW: Talk to the exchanges and understand their processes. Join industry groups such as the Blockchain Alliance. The many legitimate exchanges are more than willing to provide training, cooperate with LE and comply with the regulatory reporting regulations, and even report voluntarily where mandatory reporting doesn't yet exist. In the U.S., virtual currency exchanges have to register with the Financial Crimes Enforcement Network (FinCEN), and can be searched against the FinCEN register.

AT: ***Do you anticipate the industry will gain more acceptance from financial institutions in the future? If not, what needs to be done for the industry to gain wider acceptance?***

PW: Absolutely because this is the future and the reason that people like me are bridging the gap; I think this trend will continue.

AML PROFESSIONALS URGENTLY NEED TO RECEIVE TRAINING AND ALSO BE EQUIPPED WITH INVESTIGATIVE TOOLS

Once regulations come in, as they inevitably will, financial institutions will increasingly come onboard and those that have prepared up-front will have the advantage.

AT: ***You were instrumental in launching Project Protect in 2016, an anti-human trafficking initiative in Canada. How has Project Protect evolved since its launch and how has Project Protect been instrumental in bridging partnerships between the public and private sectors in Canada?***

PW: The project continues to deliver exceptionally with quality STRs/SARs submitted in increasing numbers, which translates to an increase in proactive disclosures by FINTRAC to LE, and increasing action by LE in a coordinated way. Aligned with this is increasing levels of awareness, and the emergence of advocacy groups about human trafficking across the community and new emerging anti-human trafficking groups. An example is Tania Ferlin of Hyatt Hotels in Toronto. She has galvanized fellow women and meeting professionals in putting on events and using social media to spread the message.

AT: ***What other partnerships or initiatives are you currently working on?***

PW: The concept of Project Protect and the public and private sectors truly working together has extended to Project Chameleon to address fraud against the elderly and vulnerable, Project Guardian to address fentanyl trafficking and more recently Project Organ, to raise awareness of organ trafficking. In my new role, I can actively extend these outreaches into the blockchain community, and I will be very much a continuing part of the ACAMS community without whom none of these successes would be what they are.

Interviewed by: Karla Monterrosa-Yancey, CAMS, editor-in-chief, ACAMS, Miami, FL, USA, kmonterrosa@acams.org

ACAMS® | Advanced Certifications

Take your AML and anti-financial crime expertise to an elevated level of education and practice.

Register today for our three-day intensive live workshop consisting of lectures, discussion and group exercises with industry experts and the CAMS community.*

*You must be CAMS Certified in order to apply.

Upcoming Live Programs:

CAMS-AUDIT & CAMS-FCI

October 15-17, 2018 | Charlotte, NC

✉ **advanced-certification@acams.org**

CAMS AUDIT
Advanced AML Audit Certification

CAMS FCI
Advanced Financial Crimes Investigation Certification

Live programs are part of the requirements to achieve the advanced certification credentials.
To learn more, visit:

www.acams.org/advanced

BORDER LESS

This past February, the U.S. Government Accountability Office (GAO) issued a report entitled "Bank Secrecy Act: Derisking along the Southwest Border Highlights Need for Regulators to Enhance Retrospective Reviews."[1] This report, which incorporates feedback from the Consumer Financial Protection Board (CFPB), Federal Reserve, Federal Deposit Insurance Corporation (FDIC), the Financial Crimes Enforcement Network (FinCEN) and the Office of the Comptroller of the Currency (OCC) presents data to support the finding that Bank Secrecy Act/anti-money laundering (BSA/AML) regulations have not kept up with legitimate risk management and cost of compliance concerns from the banking community. As a consequence, the current environment has led to a notable constriction of access to financial services in the counties along the U.S.-Mexico border.

The report, while it produces a modicum of statistical and anecdotal evidence of the challenges of accessing banking services in the border regions of California, Arizona, New Mexico and Texas, is inherently flawed due to factors presented below. Also, with the possible exception of the results of a web survey performed by the GAO, the data presented does not appear to be a statistically reliable—much less significant—sample. In addition, as pointed out by a number of the regulators, a number of relevant factors that could have reasonably been expected to impact the data were not incorporated into the analysis.

That being said, the report does profile real difficulties in accessing banking services that have reverberated through the economies of border communities.

The method to the madness

The GAO gathered information on banking account closures and restricted access to new account openings, as well as bank branch closures. This data was gathered for the 33 counties, which have 25 percent of their area within 50 miles of the U.S.-Mexico border. Statistical information was also gathered for comparable counties outside the region within the same four states, in high-risk areas elsewhere in the country and more broadly nationally.

Bank and community information

The GAO conducted a national web survey of 406 banks, including 115 from the defined southwest border region for the three-year period of 2014 through 2016. The survey, which had a 46.5 percent response rate, gathered information on account closures and limitations on new account openings related to anti-money laundering (AML) risk, the types of impacted customers, and the reasons for the closures and limitations.

In addition, three site visits were made where five discussion groups included representatives from local banks, as well as from the broader community. The three communities, Nogales, Arizona (approximate population: 20,000), San Ysidro, California (approximate population: 28,000) and McAllen, Texas (approximate population: 142,000) were chosen to provide a

[1] "Bank Secrecy Act: Derisking along the Southwest Border Highlights Need for Regulators to Enhance Retrospective Reviews," United States Government Accountability Office, February 2017, https://www.gao.gov/assets/700/690310.pdf

▲ *U.S.-Mexican border in Arizona.*

mix of urban and rural communities, different rates of branch closures, and different designations as distressed or underserved communities. Two of the discussion groups focused on retail banking customers, while the rest centered on business banking customers.

Moreover, the GAO interviewed four of the five largest border banks. Fifteen others were interviewed and selected to provide a mix of primary regulator, number of branches and asset size. Interviews were also conducted with economic development specialists, chambers of commerce, and industry and trade groups.

Regulatory information

The GAO also reviewed a spectrum of BSA/AML-related information. Bank-related data included regulatory filings of suspicious activity reports (SARs) and currency transaction reports (CTRs), enforcement actions and issues flagged during bank examinations.

In addition, documents and guidance issued by federal regulators focused on de-risking were reviewed, as were retrospective regulatory reviews, and executive orders that either proscribed or recommended such reviews.

Lastly, officials from FinCEN and bank regulators were interviewed about de-risking and retrospective regulatory reviews performed for BSA/AML regulations.

The hard (and not so hard) data

The most prominent statistical number in the GAO report is stark. Banks in the southwestern border region filed three times more SARs for each billion dollars in deposits than the national average. The overwhelming majority of banks in the region (80 percent) claimed to have terminated accounts due to BSA/AML risk, and limited or did not offer accounts to high-risk customers because of related regulatory oversight.

Background: Mexico/U.S. border region

Mexico is the U.S.' second-largest trading partner for goods, both in exports and imports. Key industries in the border region include fresh produce and manufacturing. This includes "production sharing," an arrangement where U.S. companies keep production costs down by locating some of their operations in Mexico. Border tourism is also a major economic force for border counties. In 2017 alone, three-quarters of a million pedestrians entered the U.S. at the San Ysidro border crossing, spending much of their time visiting and shopping in border communities.

The U.S. State Department considers Mexico to be a major money laundering country. The border area attracts criminal organizations for cross-border money laundering, narcotics trafficking and human smuggling, according to the U.S.' 2015 National Money Laundering Risk Assessment (NMLRA). That report also states that bulk cash smuggling is the main way drug proceeds are transported across the border. Not surprisingly, all the counties in the border regions are either High Intensity Drug Trafficking Areas (HIDTA) or High Intensity Financial Crime Areas (HIFCA), with a large majority carrying both designations.

The report notes that in the border region, high volumes of cash transactions, as well as the presence of cross-border transactions and foreign account holders contribute to the assessment of the area as higher risk for money laundering. While bank employees interviewed by the GAO say that these risks are managed by more frequent monitoring and investigation activities, they also note that these efforts require a higher investment of resources.

Adding to the AML compliance environment in the border region are the June 2010 regulations issued by the Mexico Finance Ministry. These changes put a cap on the amount of U.S. dollars that could be held by Mexican banks. Both bank examiners and FinCEN acknowledge that this altered the risk profiles of affected banks, most notably in the southwest U.S. The report explains that while (prior to the change in regulations) banks used to get cash from a limited base of Mexican banks, after the restrictions were put in place, firms had to contend with a much larger universe of individuals and companies. That change raises both the risk and the cost of compliance for the same level of business. In addition, FinCEN notes that businesses were getting more cash payments from Mexican customers, and consequently were depositing more cash (and creating elevated risk) for the banks they used.

This trend is validated through the GAO's review of CTR data: in 2016, southwest border banks filed 30 percent more CTRs than comparable in-state branches, and 60 percent more than high-risk counties outside the region.

The elevated AML risk in the region is also represented by the number of SARs filed. Banks in border counties filed three times as many SARs per billion dollars in deposits as comparable in-state counties, and two and a half times as many as in other HIDTA or HIFCA counties.

Account closures and limitations

Most border banks claimed to have terminated accounts related to BSA/AML risk. Similarly, they also did not offer accounts or they limited the number of new accounts to certain customer types consistent with their BSA/AML programs. However, the information does not provide needed details, such as raw numbers of accounts affected, or comparisons of these restricted or closed accounts compared to those affected for other reasons.

MOST BORDER BANKS CLAIMED TO HAVE TERMINATED ACCOUNTS RELATED TO BSA/AML RISK

GAO's analysis suggests that counties with a younger average age, those that are more urban in nature, those with a higher per-capita income and those with higher AML risk were more likely to lose branches. In addition, AML risks were noted as being higher in the southwest border region.

Account terminations exhibited some notable variations. While 80 percent of southwest border banks terminated accounts due to AML risk, only 60 percent of banks who also had business outside the region did. In addition, while 95 percent of large banks and 93 percent of medium banks had such closures, only 26 percent of small banks did. The report does not propose theories as to why this happened.

There were four broad categories of business accounts that were closed due to AML risk by large percentages of banks in the border region. In addition to the 70 percent of banks who closed the accounts of cash-intensive businesses, and the 58 percent who closed money services business (MSB) accounts, almost half of the banks also closed the accounts of foreign businesses, regardless of whether or not they were involved in cross-border trade.

However, the numbers of actual closures are not uniformly distributed. While 15 banks on the southwest border closed 5,396 personal accounts, and 16 banks reported 901 business accounts, one "extra-large" bank was responsible for over 80 percent (4,402) of the closed personal accounts, and slightly over half (457) of the business accounts. However, the report notes that these closures amount to less than one-half of one percent of the large bank's accounts. Similar ratios between the overall numbers and the closures by another extra-large institution exist outside the border region as well.

There appears to be a strong correlation between SAR filings and account closures. Ninety-three percent of banks on the border claim to terminate accounts due to SAR filings, although the data does not show what percentage of the closures this represents. However, three of the 19 banks interviewed required accounts to be closed based on a specific number of SAR filings, while two others claimed that the number of SAR filings caused an account review. And while yet another bank noted that SARs are one of the factors that can cause an account to be terminated, taken together, this still represents less than one-third of the surveyed institutions.

Other reasons for closing accounts that were noted in the report included customer failure to supply requested customer due diligence (CDD) information (mentioned by 80 percent of respondents), and the reputational risk associated with certain business types such as those associated with the gambling and marijuana industries (mentioned by 68 percent). While not discussed in detail, a table in the report notes that increased regulatory oversight led 63 percent of banks to close accounts, almost half cited an inability to manage the BSA/AML risks, almost 40 percent ascribed the closures to compliance costs and slightly over a quarter quoted concerns about personal liability.

Many of these factors are also noted to contribute to limitations on, or denials of, new account openings. Approximately three-quarters of banks reported such limitations or prohibitions applied to MSBs as well as all types of foreign businesses.

The report notes that failure to provide CDD information and SAR filings are the primary reasons cited for account closures outside the border region as well.

One example given for account closures points to special challenges in the border region. One bank previously offered accounts to used clothing wholesalers who exported the goods to Mexico. Mexican nationals would cross the border to buy pallets of clothes with cash, but the bank was unable to identify the source so it no longer services such accounts.

Branch closures

Branch closures in the border were not uniform; 18 counties had no closures during the report period, while five counties lost 10 percent or more of their branches. This is reflected in the three communities that the report's authors visited: McAllen lost four of 63 branches, Nogales lost a full third of its nine branches, and San Ysidro fared the worst, losing five of 12 branches.

The GAO's econometric model showed a number of interesting variations in the data:

- Urban counties were 22 percent more likely to lose branches than the most rural counties
- Counties where 70 percent of the population is younger than 45 were nine percent more likely to have closures than ones in which only one-half the population is as young
- Counties where the per capita income is $50,000 were seven percent more likely to see branch closures than ones where that figure is $20,000
- HIDTA counties are 11 percent more likely to have branch closures
- Counties where 200 SARs per billion are filed are 8 percent more likely to experience branch closures than ones that have no SAR filings

According to the GAO, many of the southwest border region's demographics are not as stark as the extremes noted above. It is roughly as urban as the national average, has a slightly lower average per capita income and slightly younger residents than the national average (60 percent vs. 55 percent). However, the report says that the border region has relatively more AML risk factors, which is reflected in the number of HIDTA counties, and the high rate of SAR filings. In fact, counties which lost branches had 10 times as many SAR filings as those which did not (600 vs. 60). However, given the relatively weak correlation between elevated AML risk factors and branch closures, there is reason to doubt that this is the cause of the closures in the border region.

Feedback from banks validates this. Six of 10 banks said AML compliance was not part of the decision to close branches, although four did say that costs (including compliance costs) could be, and one claimed that closing a branch was one way to deal with significant compliance challenges. Most tied closures to the financial performance of the branch, while three also mentioned that the volume of customer traffic and the adoption of mobile banking were also considered in the decision-making process.

Enforcement actions and regulatory oversight

From 2009 through June 2016, the southwest border counties were subject to 41 enforcement actions from regulators (in

▲ *View of the Rio Grande on the border of Mexico and the U.S. from a lookout along Farm to Market Road 170 in Presidio County, Texas. To the left is Mexico and to the right, the U.S.*

addition to two actions from FinCEN) representing 229 violations (33 percent of which were due to SAR issues, and 31 percent due to issues with controls and training). In contrast, nationally there were 576 total enforcement actions, and approximately 9,000 violations. That implies that one in 14 enforcement actions take place in the border region, and about one in 40 violations occur there.

Comments from the interviews revealed that banks tailor the nature of their businesses to ensure the avoidance of regulatory criticism. They believe that the business benefits of maintaining high-risk accounts are outweighed by the potential impact of negative comments from examiners and/or enforcement actions. Having a good relationship with regulators is important to the banks, and one person noted that they felt pressured to close accounts based on the concerns of bank examiners. Several of the interviewees stated that law enforcement and regulatory actions have made them more conservative in their approach. There was anecdotal evidence of defensive SAR filing, and one respondent claimed that his/her institution was not servicing a specific area because they were afraid that regulatory penalties could be large enough to cause the firm to go out of business. It should be noted that some of these reasons are also noted outside the border region.

This is all in line with a speech given by a Treasury representative in 2015, which noted that banks have raised concerns on the cost of compliance, as well as uncertainty about regulatory expectations and the level of potential penalties. That uncertainty leads to assuming the worst case, as the report claims that accounts are being closed not because firms are unable to manage the risks, but because the perceived costs of taking on those risks is too high. Banks perceive that the lack of supervisory and enforcement transparency increases their estimates of anticipated costs, which causes certain businesses to be considered unprofitable.

Anecdotal data

Much of the data comes from commentary from local representatives, the discussion groups and interviews. These comments provide valuable insight on unique challenges while operating in the border region:

- A regional trade group stated that border businesses prefer cash because of potential exchange rate changes while a peso-denominated check clears
- Produce industry association representatives noted that U.S. produce distributors import from Mexico and pay with a funds transfer. The exporter then withdraws the funds in cash to pay workers. This raises suspicion of

money laundering because of the timing of the withdrawal on the heels of the electronic transfer

- Some banks send staff to Mexico to establish legitimacy of businesses attempting to open accounts, while another reviews three months of bank statements to determine normal volumes of business
- Other contributors to compliance costs include translation services, and development of internal expertise on foreign identity documents
- Representatives from Southwest Border AML Alliance stated they believed some of the closed accounts were due to information from law enforcement or government agencies. The report gives the example of government guidance on funnel accounts, which led to funnel account closures.

Effects of account and branch limits

The report contains a sizable amount of information about the effects of border area banks' account closures and restrictions, and branch closures:

- A 2013 study notes that cross-border produce trade accounted for one quarter of jobs and wages in Nogales
- A business owner claimed that the volume of funds deposited from an affiliated Mexican firm caused too much risk and led their bank to close their account. It then took seven months to get a new account opened, which required coordination with banks on both sides of the border
- Economic development specialists claim that Mexican nationals spent one billion dollars in Pima County each year, and that 70 percent of sales tax is paid by Mexican customers crossing the border to shop. However, they make fewer trips now, because accounts in U.S. banks that they use to withdraw funds for their shopping trips are harder to maintain. This, in turn, affects the economies of border communities. Similarly, branch closures lead to less foot traffic that depresses sales volumes, as evidenced by changes in the fortunes of businesses along San Ysidro Boulevard in the wake of branch closures
- Similarly, lost branches reduce means of borrowing, which limit investments in local communities. For example, Tucson businesses have turned to alternative funding sources, including loans from family members, title loans and accounts receivable lending. This is also validated by academic research that finds that closures lead to reduced small business lending as well as employment growth in the immediate area
- Branch closures cause people to travel further to conduct banking activities, to pay higher fees for using alternatives for their financial services, and increased difficulties completing their transactions. People in Nogales and San Ysidro have to travel between 20 and 40 minutes to the nearest bank branch, although one person noted that they travelled over 70 miles to another branch of their bank because they were afraid they would not be able to open an account at another bank

Regulators respond

The regulators that were consulted for the report provided feedback on the initial draft of the report, and their feedback was incorporated in, among other places, a separate section of the report. The feedback largely focused on two areas: the steps being taken to address the issues, and pointing out flaws in the report and its methodology.

A 2013 STUDY NOTES THAT CROSS-BORDER PRODUCE TRADE ACCOUNTED FOR ONE QUARTER OF JOBS AND WAGES IN NOGALES

For example, the FDIC mandated that examiners document the instances where they recommend account closures. However, as of December 2017, no closures had been recommended.

Multiple statements by the Financial Action Task Force (FATF), the OCC and FinCEN have addressed the need to balance AML compliance with the need for financial inclusion and access. However, the GAO responded by saying that the actions taken by regulators do not consider all factors and, the regulatory reviews that they perform are not broad enough.

FinCEN responds

FinCEN did not get their response to the GAO in time for it to be included in the final report. However, it responded in a separate memorandum.

FinCEN deems the problem of de-risking to be important, and claims to have been actively addressing it by clarifying what drives it and how it can be addressed.

They also participate in multiple governmental initiatives. These include the Multi-State MSB Examination Taskforce, the Conference of State Banking Supervisors, the Federal Financial Institutions Examination Council, the Financial Stability Board's Correspondent Banking Coordination Group and the promulgation of the 2014 Money Remittances Improvement Act. De-risking is also a major focus of the BSA Advisory Group.

FinCEN believes that restricted access to financial services is due to a misunderstanding by firms of their compliance responsibilities.

FinCEN also had a number of criticisms of the GAO report and its methodology. Perhaps the most fundamental is that GAO's definition of de-risking is not the standard one. A consequence of this is that the report does not differentiate restrictions imposed based on individualized assessment of account risk, as is the recommended norm, from restrictions imposed due to de-risking, which is the uniform treatment of entire classes of customers with common characteristics. By doing so,

the report implies that the compliance requirements themselves are the cause of all perceived account restrictions.

Similarly, the report does not define when regulatory concerns justify account closures, nor does it explain how the GAO determines when regulatory oversight is proper.

FinCEN also notes that the higher levels of SAR and CTR filings may be partially due to the Mexican currency control restrictions, as well as financial activity performed as part of criminal activity. As the report does not attempt to quantify these effects, it is impossible to gauge what portion of the filings are defensive, and which are justifiable on the merits. Similarly, the memo notes that the report fails to leverage law enforcement data or their perspectives on financial crime in the border region, as well as more broadly.

In fact, the memorandum also notes that there is an ongoing trend of branch closures in less densely populated areas that is consistent with the higher rates of branch closures in Nogales and San Ysidro as opposed to that in McAllen. FinCEN notes that if branches were being closed due to BSA/AML concerns, the number of CTR and SAR filings would have decreased—but they have not.

At a basic level, FinCEN concludes that the GAO analysis does not show that the loss of access to financial services in border regions has occurred at a higher rate than elsewhere.

Is the truth in the middle?

If one considers the identifiable trends in the data, both quantitative and qualitative, some things are clear. Whether it meets the standard definition of de-risking or not, there is an identifiable impression of higher standards for opening or maintaining an account that appears to be linked to anti-money laundering/counter-terrorist financing program requirements, and the fear of receiving adverse BSA/AML-related comments in a regulatory examination. The change in the Mexican currency controls, and the attendant shift from receiving cash from a relatively small number of known financial institutions to dealings with larger sets of individual consumers who are more difficult and more expensive to perform due diligence on, amplifies those concerns in the southwest border region.

One thing should be clear: creating financial services "deserts" is not only not in consumers' interests, nor that of the communities in which they live, it is counterproductive to the goals of regulators and law enforcement officials who are trying to identify, trace and stop financial crime. When traditional financial services firms are not readily accessible, money launderers do not stop their illicit activities. They either find outlets in other communities, merely shift the risk geographically or they find alternative means of moving money, at least some of which will not provide the same level of traceability and oversight as traditional service providers.

How might the higher level of BSA/AML-related closures and restrictions be more effectively addressed? It might help, as noted in the Treasury speech as well as comments from the public noted earlier, to have greater clarity on regulatory examinations and the standards needed to be applied. In addition, perhaps the standards should not only provide a sense of what is considered too lax, but also what is considered to be overly restrictive, absent extraordinary circumstances.

Similarly, if FinCEN and bank regulators issued clear, yet flexible, enforcement guidelines—with clearly spelled-out gradations of response and factors considered in the decision-making process—banks along the southwest border (as well as elsewhere in the country) would have less uncertainty about whether or not the efforts they are undertaking will be deemed adequate and, if they are considered to be inappropriate, how that is reflected and managed by regulators.

In a more general sense, maybe what is needed is a paradigm shift for regulation and oversight: from mandating and ensuring that firms have an "effective" BSA/AML program to requiring one that is truly "appropriate" for the individual institution. Such a change would likely slow the rate of unnecessary BSA/AML compliance-related denial of services, better rationalize the risk tolerances and costs of compliance for regulated firms, and keep more criminal assets in traditional financial services firms, where they can be identified by banks, and subsequently interdicted by the authorities.

Eric A. Sohn, CAMS, director of business product, Dow Jones Risk & Compliance, New York, NY, USA, eric.sohn@dowjones.com

▲ *Border Field State Park beach in San Diego, California with the international border wall separating the U.S. from Tijuana, Mexico.*

ACAMS® | Certificates

Get compliance trained and prove your commitment to protecting your institution against financial crimes.

Earn your training certificate

www.acams.org/certificates

CHEATERS NEVER PROSPER

Every level of society faces corruption. It is a worldwide issue that affects every country to some degree. Transparency International publishes an annual "Corruption Perceptions" Index that ranks countries from least to most corrupt.[1] Corruption does not discriminate. It touches both the public and private sectors. Public corruption ranges from the senior-most levels of government to the junior levels. It involves elected officials, as well as government and municipal officials and employees. Private sector corruption includes corporate or business corruption, union corruption and corruption involving non-government agencies. Corruption also includes individuals paying bribes in both public and private sector settings.

"Corruption has a corrosive effect on the rule of law, economic development and democratic principles. It is a threat to national security."[2] Corruption undermines trust in the government and serves as an incubator for terrorists and transnational criminal organizations. It is a threat to public safety. Corruption weakens the infrastructure and systems of governance. It is a threat to the economy. Corruption undermines legitimate financial flows and adversely impacts legitimate business. Corruption and bribery are often difficult to identify and challenging with which to deal. Money laundering is an essential component of corruption. Individuals and entities engaged in corruption must have the means to move ill-gotten gains through the financial system in a manner to avoid detection.

In most instances, individuals engaged in bribery and corruption endeavor to take careful steps to avoid detection. There are many mechanisms available to blur transparency and obscure corrupt activities. Although the range of public and private sector corruption is vast, there is one constant. That constant is money. Invariably, illicit payments are exchanged. Financial institutions serve as a detection mechanism or a facilitation tool. The flow of illicit funds generated as a result of bribery and corruption will pass through financial institutions. From an anti-money laundering (AML) risk perspective, what do you think of when you hear about bribery and corruption? Most AML professionals would think about politically exposed persons (PEPs) and the risk of banking corrupt PEPs.

Would you think about corruption in sports? When compared to PEPs, threats to national security, public safety or national economies, would you consider corruption in sports to be a significant problem? Why should AML professionals be concerned about corruption in sports? One important reason would be if your financial institution served as a facilitation tool for corruption in sports. That would be especially true if your financial institution served as a facilitation tool for serious systemic sports corruption such as the FIFA scandal that came under public scrutiny on May 27, 2015. On that date, the U.S. Department of Justice (DOJ) held a press conference to announce the criminal indictment of 14 highly ranked officials and corporate executives affiliated with FIFA. In addition, it was announced that related guilty pleas of four additional individuals and two corporate defendants had been unsealed.

FIFA is the Federation Internationale de Football Association. It is the world governing body for international soccer. The FIFA scandal was covered in more depth in the September-November 2015 issue of *ACAMS Today* magazine, the article was titled *The World Cup of Fraud*.[3] There had been long standing allegations about the widespread culture of corruption ingrained throughout FIFA at the highest levels of governance. What is noteworthy from an AML perspective is that the indictment named at least 27 financial institutions that held conspirator accounts. At the time, the acting U.S. Attorney for the Eastern District of New York, Kelly T. Currie, stated that the investigation would look at financial institutions that facilitated bribe payments, and money laundering to see if the institutions were cognizant of the fraud. Shortly thereafter, the Financial Action Task Force issued a statement indicating that it did not appear that financial institutions gave a sufficient amount of scrutiny to the financial activities of the officials engaged in bribery and corruption schemes.[4]

Looking at corruption in sports more broadly and taking a step back, it should be noted that corruption can be traced back to the origin of sports. Throughout the years, as the business of sports has gained greater economic prominence, the opportunity for enrichment through sports business corruption has grown exponentially. Corruption is the abuse of entrusted power for personal gain. This is true in sports as well as other private and public corruption activities. Corruption in sports comes in a variety of activities ranging from match-fixing, illegal gambling, doping, rigging the awarding of the bidding process to host major sporting events, to steering athletes to endorsement contracts and player agents. When assessing the significance and impact of corruption, it is important to determine if the corruption is systemic or one-off in nature or if there are a series of one-off incidents that point to a weakness or vulnerability that leads to systemic exploitation.

[1] "Corruption Perceptions Index: Overview," Transparency International, https://www.transparency.org/research/cpi

[2] Dennis Lormel, "How Money Laundering and Corruption Impact the World Economy," Institute for Fraud Prevention, http://theifp.org/documents/Corruption-Illicit-Financial-Flows-and-Money-Laundering.pdf

[3] Dennis Lormel, "The World Cup of Fraud," *ACAMS Today*, August 25, 2015, https://www.acamstoday.org/world-cup-of-fraud/

[4] Ibid.

A good example of a one-off incident of sports corruption is the 1919 Black Sox scandal. The Black Sox scandal involved Major League Baseball. Eight players on the 1919 Chicago White Sox were accused of accepting bribes to intentionally lose the World Series against the Cincinnati Reds. The players resented team owner Charles Comiskey because despite being the best team in baseball, they were one of the lowest-paid teams. One of the players who allegedly took part in the bribe scheme was Shoeless Joe Jackson, one of the greatest players of the era. He was banned from baseball and denied entry into baseball's Hall of Fame.

An example of a series of one-off incidents that point to a weakness or vulnerability in the system is in European soccer, or football. In this case, referees and/or players are periodically bribed or offered bribes to fix matches. This is a recurring problem. In response to this problem, the Union of European Football Association (UEFA) teamed up with Europol by signing a memorandum of understanding to investigate allegations of match-fixing in Europe. Europol is the European Union's (EU) law enforcement agency. UEFA is one of six FIFA regional organizations. UEFA represents the national football associations of Europe and is most prominently known for the UEFA Champions League, which is comprised of the top club teams in each European League. It is an annual competition where the winner is awarded the European Cup. The European football leagues and UEFA competitions are quite numerous, passionately followed by fans and extremely lucrative. These dynamics make them particularly susceptible to match-fixing.

No sporting competition is as lucrative and passionately followed as the FIFA World Cup. The 2018 World Cup for men's teams is scheduled for June 14 to July 15, 2018. Russia is the host country. Thirty-two teams will compete in a total of 64 matches held in 12 venues across 11 cities. As the host country, Russia received an automatic bid. The other 31 teams competed in regional competitions around the world involving the 209 FIFA member associations. The qualifying tournaments began in 2015. Notable countries that failed to qualify for the 2018 World Cup included Italy, Netherlands, Cameroon, Chile, the U.S. and Ghana. Among the excitement and anticipation as the competition draws closer, a dark cloud hangs over the 2018 and 2022 FIFA World Cups. There are strong allegations—and evidence to support such allegations—that the bids to host the 2018 World Cup in Russia and the 2022 World Cup in Qatar were rigged. This leads us back to the culture of corruption in FIFA.

> THE POOR TONE AT THE TOP OF FIFA AND THE CULTURE OF CORRUPTION LEADS TO A SLOW AND INCREMENTAL PROCESS IN CHANGING THE CULTURE OF COMPLIANCE

FIFA's longstanding culture of corruption was never more evident than in the aftermath of the DOJ press conference on May 27, 2015. Then FIFA President Sepp Blatter was highly critical of the DOJ investigation. Two days after the press conference, on May 29, 2015, FIFA's congress reelected Blatter as president. As noted in *The World Cup of Fraud*, "Blatter's reelection demonstrated FIFA's culture of arrogance and indifference to corruption."[5] The investigation being conducted by the FBI and the U.S. attorney's office for the Eastern District of New York would be a long-term investigation resulting in more criminal charges. The poor tone at the top of FIFA and the culture of corruption leads to a slow and incremental process in changing the culture of compliance. So, where are we now in May 2018, approximately three years after the FIFA indictments were announced and (at the time of this writing) on the verge of the 21st FIFA World Cup tournament commencing in June 2018?

The criminal investigation being conducted by the FBI and DOJ is ongoing. One important aspect of the investigation is that no financial institutions have been found to be criminally culpable or negligent. As of the end of April 2018, at least 41 individuals and/or companies have been criminally charged. Twenty-five of those charged have been convicted in the U.S. Sepp Blatter was removed as president of FIFA in December 2015. Gianni Infantino was elected by FIFA's congress to succeed Blatter as president on February 26, 2016. Infantino after his appointment said he is committed to reforming FIFA and establishing good governance and transparency. Even if he could achieve these aims, the stench of corruption in FIFA will last a long time, and changing the culture of corruption will continue to be an incremental process. The jury is out on whether Infantino will succeed. FIFA did not help itself in reducing skepticism when they refused to reconsider holding the 2018 and 2022 World Cups in Russia and Qatar, respectively, in spite of the allegations and evidence of rigging the bids.

FIFA does not have a monopoly on systemic corruption in bid rigging and contract manipulation in sports, the U.S. National Collegiate Athletic Association (NCAA) is guilty of corruption as well. Much like the undercurrent of corruption that has long plagued FIFA, the NCAA has consistently avoided the issue of collegiate amateurism and the institutional exploitation of college athletes by businesses and colleges. Most notably, since 2016, NCAA college basketball has generated a billion dollars per year in television contracts. During the basketball season, the NCAA holds numerous tournaments. At the end of the season, most college conferences hold conference championship tournaments. This leads to what is referred to as "March Madness." March Madness is the college basketball national championship tournament. It is a single elimination tournament involving 68 Division I colleges. There are approximately 300 Division I college basketball teams. The tournament is a media-intensive event that generates significant revenue for participating schools, conferences and business

[5] Ibid.

interests. The 2018 national championship tournament ran from March 15 to April 2, 2018, when the national championship game took place.

On September 26, 2017, the FBI and U.S. Attorney's Office for the Southern District of New York announced the indictments and arrests of 10 individuals associated with NCAA college basketball. In the aftermath of the indictments, Hall of Fame basketball coach Rick Pitino was fired by the University of Louisville for being linked to alleged illicit payments. Pitino has not been criminally charged in the ongoing investigation. Those charged were four assistant college coaches, three athletic advisors, one senior executive of Adidas and two other individuals affiliated with Adidas. Adidas sells athletic shoes and apparel and relies on player endorsements of their products to generate considerable income. The 10 individuals indicted were charged in bribe schemes.

Illicit payments were funneled to elite players and/or their families to steer them to schools sponsored by Adidas. This was primarily done through Amateur Athletic Union (AAU) basketball teams sponsored by Adidas. Although not charged in the indictment, it is alleged that Nike and Under Armour, competitors of Adidas, engage in similar activities. Once the players were steered to the select schools, the assistant coaches received illicit payments to steer players, on the verge of turning professional, to specific player agents or advisors, and to encourage them to sign endorsement deals with the school-sponsored shoe company.

Although the indictments were announced in September 2017, it was well known that players were steered from AAU teams to college programs sponsored by the shoe companies that also sponsored the AAU teams. Then, when the players turned professional, the shoe companies would steer them to specific agents and shoe endorsement deals. Many coaches and college administrators turned a blind eye to these practices. A good analogy for AML professionals is that coaches and school administrators were willfully blind. As a result of the indictments and pervasiveness of the scandal, NCAA President Mark Emmert appointed a 14-member Commission on College Basketball. The commission is chaired by former National Security Advisor and Secretary of State Condoleeza Rice.

As the NCAA national basketball tournament was about to start, media reports surfaced that the FBI investigation identified 25 current and former college players who benefited from illicit payments. Prominent coaches and/or colleges have been named for having players who received illicit payments. All indications are that the FBI and the U.S. attorney's office for the Southern District of New York are engaged in a long-term investigation that will result in additional charges being brought against more individuals and companies.

On April 25, 2018, Rice issued a report making a series of recommendations for rule changes in NCAA college basketball. In calling for greater accountability and stiffer NCAA penalties, Rice stated in a news conference, "Bad behavior is too often ignored and inadequately punished." In a joint written statement with two other NCAA officials, Mark Emmert noted, "This is about more than college basketball. This is about the culture and future of college sports. We will all work together to get it right." The question is, will the NCAA get it right? As with FIFA, the NCAA has a culture of indifference. Only time will tell.

From an AML perspective, illicit funding flows in the FIFA scandal range from the hundreds of thousands to millions of dollars. The illicit funding flows in the NCAA scandal range from thousands to about $150,000. How likely is it that financial institutions can identify the illicit flow of funds in either scandal? The FIFA scandal has been ongoing for three years. The NCAA scandal has been ongoing for a little over seven months. In both cases, negative news would be more likely to generate alerts than transaction monitoring would. There is also the possibility that law enforcement requests for information, either through legal process, such as the statement of facts in the indictments, subpoena service and/or 314(a) requests would trigger alerts. More is known about typologies used in the FIFA scandal and the dollar amounts are much more significant. Most FIFA executives were not PEPs but should have been considered PEP-like and high-risk customers after the scandal surfaced. In the NCAA scandal, it would be extremely difficult to categorize anyone as being PEP-like or high risk.

As these scandals play out, financial institutions should follow media reporting and the law enforcement investigations closely. Financial institutions should pay close attention to potential touch points they may have to one or both scandals with individuals or businesses who may have been engaged in illicit activity. The author is a strong proponent for financial institutions establishing special investigative teams to deal with these types of matters. In a number of articles and presentations, these special investigations teams are likened to law enforcement Special Weapons and Tactical (SWAT) teams. SWAT teams are specially trained to handle and resolve extremely dangerous situations. Similarly, if financial institution special investigations teams received specialized training, then they would be better equipped to deal with significant and sensitive situations.

The FIFA and NCAA scandals are both serious systemic problems that have adversely affected sports. They were both long time problems that were tolerated and not adequately dealt with. Although these scandals do not cause national security or public safety concerns, they do cause economic stress and adversely impact legitimate interests by causing an illicit, unfair advantage to individuals and businesses engaged in and benefiting in corrupt activity. Financial institutions should assess the potential likelihood that they could be a facilitation tool and determine how they could be a detection mechanism by understanding illicit funding flows and the typologies used by actors complicit in the two corruption scandals.

Dennis M. Lormel, CAMS, internationally recognized CTF expert, president & CEO, DML Associates LLC, Lansdowne, VA, USA, dlormel@dmlassocllc.com

Sports Corruption Place

TUNING UP BSA/AML

When it comes to the Bank Secrecy Act/anti-money laundering (BSA/AML), law enforcement needs to be better financial institution translators (FIT). While their private sector counterparts have invested substantial resources, time and effort in the latest analytical software, systems and advanced training in BSA/AML, too much of law enforcement has lagged behind. Historically, innovative changes in law enforcement have always been slow. However, there is no "old school" in cyber technology. The analytics that are commonplace in modern BSA/AML compliance are not always commonly known by the law enforcement entities who are expected to undertake the investigative actions envisioned by BSA/AML compliance departments. This communication gap is repairable, but it requires an adjustment to "old school" thinking in all the sectors that comprise BSA/AML.

A key issue here is that there is too much "assuming" that goes on. Mostly, it is various sectors of BSA/AML assuming incorrect information or motivations of the other sectors. One of the most detrimental assumptions is that your average law enforcement investigator is as knowledgeable about the BSA/AML efforts and innovations as are their counterparts in financial institutions.

Assumptions like these survive the same way many money launderers survive; the facades they present are thin, but you still need someone to look below the surface to challenge them. The standard, and very predictable, law enforcement response to the private BSA/AML compliance sector is to compliment and thank them for all their hard work. Although that is typically followed by expressing the important role that suspicious activity reports (SARs) have allegedly played in investigations, true empirical data supporting the veracity of that is harder to obtain.

Most people will concede that the large majority of criminal activity is committed for, or with, financial motivations. Compare that to the total amount of all law enforcement investigative resources, efforts and energies that are devoted to the financial aspects of investigations and you will find quite a disparity. Certainly there are many valid and proven reasons for this disparity. Abating the violence that scoundrels will employ as part of their schemes to enrich themselves is, and should be, a priority over the loss of money or property. The Bank Secrecy Act (BSA) puts an investigative strategy and priority on following the money. Public safety continues to be the primary law enforcement investigative strategy. In some cases, the interdiction of illicit activities after the financial transactional phase may actually offer a way to reduce or minimize some of the public safety concerns. When and where things like drugs and money change hands creates various levels of public safety concerns. Interdicting a crime "in progress" can create a dangerous and emotionally charged situation. Interdicting the crime from the financial irregularities created by those illicit activities may minimize some of these public safety concerns.

Mixed results might be the most optimistic assessment of whether law enforcement has lived up to its perceived role in the BSA/AML effort. From the start there was a lot of assuming that law enforcement careers and experiences primarily abating crime from the public safety aspects would quickly adapt to shifting primary concentrations to the financials. The numbers had always fallen in place because they dovetailed well with the other unlawful activities on which the investigations had focused. The drugs or other dirty deeds mixed together with the money requires only minimal financial analysis. Doing that in reverse became more akin to trying to recite the alphabet in reverse. Since there is still enough of the "in progress" interdictions, law enforcement can, and often does, simply put a BSA/AML label on some cases when the money or other assets recovered have the better optics. Procrastination in having to actually get up to speed with the rest of BSA/AML is commonplace within law enforcement. The "follow the money" banner is spoken about far more than actually practiced.

Financial institutions only had the financial side. They had to embrace an investigative approach from that aspect. The considerable resources and efforts devoted to having advanced analytical software and programs for identifying and combating money laundering and financial crimes made them excellent at it. To understand how behind much of law enforcement is, you just need to look at what is routinely and regularly accepted by law enforcement as the required "supporting" documents to SAR filings. With all these analytics and resources being devoted to BSA/AML compliance, oftentimes just a couple statements, without context or relevance, will be sent in response to these law enforcement requests. That would almost be laughable except for the fact that those responses are rarely challenged. What it does reflect is the serious communication gap between the two sides. This lack of having the totality of what truly "supports" a SAR filing may change or impede investigative decisions before a viable investigation is even undertaken.

What exasperates this problem is how the functions of many BSA/AML compliance sections are not even well known within the financial institutions of which they are a part. When that is true for the subpoena or legal order processing departments, viable investigations will suffer. Those departments have been around long before the BSA and have assisted law enforcement when the financial institutions supported

traditional investigations. They rarely relied on in-depth analytics of the transactional data required in many potential money laundering cases. Nuances in know your customer and comparable analytics had never been an issue before. Money laundering investigations are often made or broken with nuances and small mistakes found in the fusion of all aspects of a suspect's activities. What a financial institution may consider an innocuous internal bank communication or document may actually help show intent, confirm or even contradict other information or data an officer or agent may have (assuming they would have no relevance and not sending them can seriously undermine investigations). Speak to any experienced investigator and you will quickly learn how many "little things" ended up breaking their biggest cases.

Many subpoena compliance or legal order processing departments have developed regimented responses as to what is produced or supplied. Even when nearly every conceivable record or document is articulated within a subpoena request, the initial response is normally to send a superficial packet of the easily accessible and the most commonly known bank documents. If an agent or detective is ignorant or unaware that there is substantially more information, to include the BSA/AML information, those responses will not be challenged. Those detailed analytical spreadsheets and other investigative efforts by the BSA/AML compliance section are never used for their designed purpose. What is the intent of the BSA in regards to this?

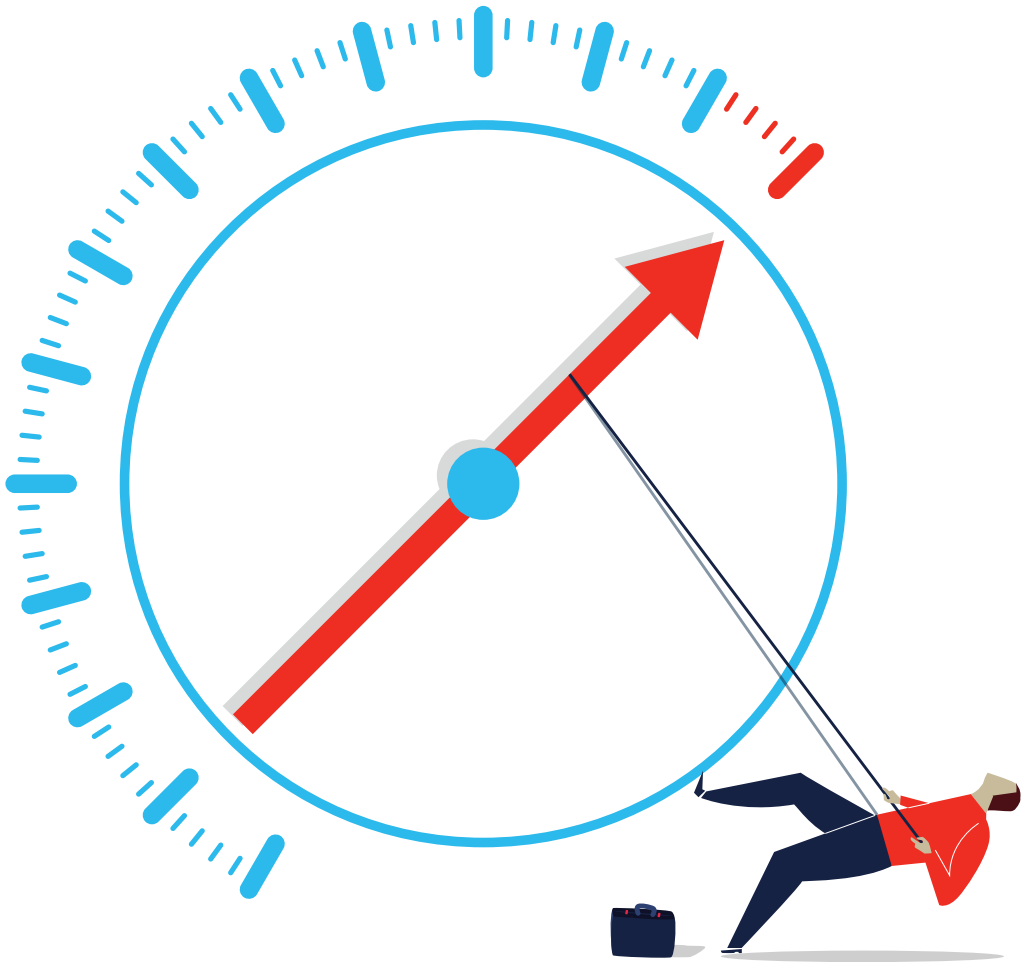
A public-private partnership is essential and indispensable in the anti-money laundering (AML) fight. There is no doubt that more in law enforcement need to be better FIT to fulfill their role in this partnership. In the interim, those in BSA/AML compliance should educate, translate and never assume their efforts are being properly communicated. If information or intelligence is collected, it needs to be used or disseminated for the reason it was collected. If you believe something is too confidential to ever be used or disseminated for the very reason it was collected, you are doing this wrong.

Money laundering will never be fully eradicated but certainly a lot more can be done to abate it if we can get BSA into better shape!

There is a lot to work out! I assume you agree.

Steve Gurdak, CAMS, supervisor, Washington Baltimore HIDTA, Northern Virginia Financial Initiative (NVFI), Annandale, VA, USA, sgurdak@wb.hidta.org

Disclaimer: The views expressed are solely those of the author and are not meant to represent the opinions of the W/B HIDTA.



A post-task force paradigm: The community of interest

"It may be that, in the strategic context of a particular jurisdiction, more than one model can be adopted to deal with different issues or geographic levels of information sharing, rather than having an overarching national [Financial Information Sharing Partnership]."[1]

A complex criminal ecosystem exists in Southern California and like the seismic fault lines beneath us, criminal actors cross jurisdictions with malevolence and stealth. Clever and committed people are required to contain these forces and to mitigate the financial impact of their crimes. The stability and well-being of the financial sector is of paramount importance. While food, water and shelter are requisites for survival, the integrity of our economic infrastructure is a critical pillar for societal health.

Pursuant to the Money Laundering and Financial Crimes Strategy of 1998, particular geographic areas and industries are at a heightened risk, both qualitatively and quantitatively, to the commission of money laundering offenses. Southern California is one of seven regions across the U.S. designated as a High Intensity Financial Crime Area (HIFCA). In its present form, the Southern California HIFCA is comprised of seven counties: San Luis Obispo, Santa Barbara, Ventura, Los Angeles, Orange, Riverside and San Bernardino. Locally, this criminal ecosystem is manifested in different threat sectors that present unique enforcement challenges. These sectors include, but are not limited to, the wholesale district (garment, jewelry, toys and flowers), gambling, narcotics, white collar, informal value transfer systems, ethnic organized crime, cyber and import/export. Considering various factors, such as the type and scale of importations (sea, land and air), geographic area, diversity of industries and ethnic populations, this region is vulnerable to the most challenging schema devised by perpetrators of myriad specified unlawful activity.[2]

Mutual support among public and private sector stakeholders is vital and an easily identifiable network is critical to marshal interoperable components and conserve resources. Homeland Security Investigations (HSI) Los Angeles, the Internal Revenue Service—Criminal Investigations Los Angeles (IRS-CI) and the U.S. Attorney's Office for the Central District of California (USAO) sponsor the Southern California HIFCA and have dedicated partnership from the California Department of Justice's Bureau of Gambling Control (BGC). Collectively, the Southern California HIFCA represents our commitment to lead the effort to enable our community's financial crime enforcement.

Of course, the aim toward joint enterprise and collective betterment is a worthwhile endeavor. To this end, HIFCA is seeking to embolden existing relationships by introducing a new operational model for multilateral engagement. This model is more amorphous, less focused on promised commitment and the memorandums of understanding concomitant with traditional partnerships, such as the ubiquitous "task force." Here, we look to a community of interest (COI), which in this context is focused on the anti-money laundering (AML) efforts committed to combating financial crime in Southern California.

A COI is a forum where shared interests, information and techniques can be exchanged by a group focused on a common goal or cause. Ontologically, a COI is different, but not wholly unrelated or mutually exclusive, from the task force model where agencies formally agree to a mission and allocation of resources. Unlike a task force, a COI does not condition support on participation. In the task force pay-to-play framework, stakeholders can be shut out and information flows constricted. In addition, a sort of localism frequently attaches and foments parochial, proprietary attitudes that create friction with the larger community. A task force must continually reinforce its purpose through attributed action and defined metrics. In a COI, there are no objective criteria to gauge success because a benefit is subjectively measured by each member.

The COI is branded as El Camino Real with an eye to its California roots, its symbol as a pathway to a new order and as a homage to the El Dorado Task Force in New York.[3] El Camino Real represents the confluence of investigative and intelligence groups, coupled with digital modes of communication. Presently, HSI, IRS-CI, USAO and BGC have nine investigative groups, one intelligence unit, forensic accountants and an assistant

[1] Nick J. Maxwell and David Artingstall, "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime," Royal United Services Institute, October 2017, 33.

[2] Specified unlawful activity enumerated in 18 U.S. Code Sections 1956(c)(7) and 1961(1) define the predicate criminal acts that are required to substantiate a money laundering offense.

[3] The El Dorado Task Force (EDTF) is a HSI-led financial crime investigative/intelligence initiative headquartered in New York City that began in 1992. EDTF is the model for many similar efforts, to include this one.

U.S. attorney dedicated to this effort and looking to offer these assets to our fellow stakeholders.

The COI will act as a networking platform where members can be identified, information is shared and requests for assistance are made. The COI will interface with its law enforcement partners through a secured online portal, referenced as the El Camino Real Switchboard. In the spirit of the homeland security enterprise, HIFCA will seek nominations of personnel from all the federal, state, local and tribal law enforcement agencies in its area of responsibility. The nominees will be the internal and external points of contact for their respective agencies and act as the portal for communications regarding financial crime affecting their area of responsibility. The purpose here is to smooth out the pathways of communication. The knock-on effects will include a reduction in effort expended to identify our partners and develop subject-matter experts who will have a holistic vantage of the financial crime activity in their area of responsibility (AOR).

Law enforcement members of El Camino Real will use HIFCA's agents, analysts and forensic accountants as an investigative support system and resource base. For example, HIFCA has near real-time access to the Financial Crimes Enforcement Network (FinCEN) Suspicious Activity Report (SAR) database.[4] Our analysts can access and analyze SAR data for departments that might not have the capability or familiarity with the process.[5] Because El Camino Real is a COI and not a database or deconfliction portal, SAR data will not be stored on it, so dissemination will not violate FinCEN's use of data precepts. The information shared within and without the COI will be no different from what is or can be shared currently. The COI merely creates an easier way to identify other financial investigators, seek assistance and obtain information. Law enforcement partners will want to participate in El Camino Real because it promotes their mission and requires no outlay of resources.

HIFCA is well-positioned to establish and lead the COI. As a large federal investigative agency, HSI has an expansive jurisdiction, strong national presence and broad international reach. The ethos of HSI, vis-à-vis the Department of Homeland Security (DHS), is to collaborate and share information/resources. DHS was shaped in the post-9/11 spirit to breakdown stovepipes and promote integrated networks.[6] HSI's focus on poly-crime and transnational actors, coupled with the unique jurisdiction of IRS-CI, enables the two to gather information and enforce laws that no single government agency can. With the powers of the USAO and BGC, HIFCA has the ability to pursue criminal, civil and administrative actions on the federal and state level.

Augmenting HIFCA's effort to combat crime within the specific threat sectors and specified unlawful activity (SUA), such as human trafficking and smuggling, counterterrorism, child exploitation, contraband smuggling and munitions trafficking, El Camino Real will promote specific projects that traverse both segments. Currently, there are four projects. However, this is an area that is primed for community input.

Divining Rod

Project Divining Rod is a public-private sector enterprise aimed at the strategic production and proactive data mining of SARs pertaining to HIFCA threat sectors and SUA. SARs are the lifeblood of countless criminal investigations. Pursuant to the Bank Secrecy Act (BSA), financial institutions must establish AML programs.[7] The generation of SARs is an expression of their compliance. Because financial institutions cultivate the data that law enforcement relies on, it is incumbent on law enforcement to orient them to its investigative focus so they can opt to recast their resources to support law enforcement's mission.

[4] FinCEN is part of the U.S. Department of Treasury and is empowered by Congress to collect, analyze and disseminate data collected under the statutes and regulations that collectively and colloquially compose the Bank Secrecy Act: https://www.fincen.gov/what-we-do

[5] The sharing of SAR data is conditioned upon recognition and acceptance of the restricted use of SAR data, which will be detailed to members during the nomination/validation process.

[6] DHS was created pursuant to the Homeland Security Act of 2002, https://www.congress.gov/bill/107th-congress/house-bill/5005]

[7] 31 U.S. Code Section 5318(h)(1) and 31 Code of Federal Regulations Section 1020.210 mandate that financial institutions implement and maintain AML programs to include "ongoing monitoring to identify and report suspicious transactions."

In the AML realm, the private sector's main criticism of law enforcement is the lack of feedback they receive on the SARs they file. Feedback is an enabling element in a relationship founded on planning, collection, analysis and dissemination.[8] It has been law enforcement's oversight not to be more effective in this area. One reason law enforcement has minimized the importance in providing feedback derives from its normative use of SARs as a retroactive investigative tool. Inherent in retroactive use is the temporal attenuation between the author and the user of the SAR as well as timidity and/or difficulty in making contact. Once SARs are recognized as valuable proactive tools, feedback is seen not as the last step in the cycle, but the first.

In the context of the COI, the public-private and private-private sector relationships are not as cohesive as the public-public relationship. Namely, financial institutions are not as homogeneous or united in mission as the police. Hopes that Section 314(b) of the USA PATRIOT Act would instill an esprit de corps amongst financial institutions—without law enforcement as a catalyst or intermediary—are beneficently aspirational, but most likely illusory in a capitalist economy.[9] The common denominator financial institutions share is the pressure to comply with the mandates of Section 5318 of Title 31.[10]

It is important for law enforcement to recognize the private sector's pressure points. AML mandates seemingly demand that they know tomorrow's everything yesterday while trying to reconcile law enforcement's goal to control crime. We are partners, at least in the BSA/AML space, with parallel interests albeit divergent missions. There is common ground not yet occupied, but groundbreaking efforts are taking hold at the national and supranational level.[11] Law enforcement needs to recognize the private sector's desire for direct participation and recognition of effort since they act as de facto intelligence cells for our investigations.

Financial institutions are interested in what we do and seek direction in proactive targeting. El Camino Real seeks to enable more efficient and broader use of SARs by offering financial institutions a direct pathway to investigators/analysts. Currently, much of the public-private discourse is procedural (i.e., a response to 314(a) request) or at not easily accessed top-official levels. El Camino Real will offer a mechanism to receive direction and feedback from law enforcement and vice versa. The direct connection will be accomplished by the publication and presentation of materials like this within BSA/AML fora. Part of this process will include an invitation to the private sector to submit summaries of SARs directly to HIFCA intelligence analysts who will review the SAR data with a focus on the articulated threat sectors and SUA. The SAR summaries can be emailed to ElCaminoReal@ice.dhs.gov. The following are a couple of examples:

SAR ID 0000123456—XYZ Inc.

XXX, a retail bank, is filing this SAR for $25,530,075.02 in Automatic Clearing House (ACH) wire transfer deposits on the business checking account, #10987654321, of XYZ, Inc., located at 501 W. Ocean Blvd., Long Beach, California, whose source is unknown, giving the appearance of money laundering. Additional suspicious activity occurs in the form of ACH withdrawals, which are conducted by XYZ to at least 15 different domestic credit card issuers and business checks to approximately 25 different individuals with addresses in as many states. This activity was conducted from May 2, 2016 to March 3, 2017, and includes the company owner John Doe (DOB: January 1, 0000, SSN: 123-45-6789) and bank customer Jane Doe (DOB: January 1, 0000, SSN: 123-45-6789).[12] This activity is considered suspicious primarily as the source of the ACH deposits is unknown, it appears excessive for the expected activity regarding an account of this type and business of this size, it appears to consist of activity with little to no business, economic or lawful purpose, and is potentially reflective of trade-based money laundering. Information provided by the customer upon account opening regarding the expected activity reflects a significant difference to the activity observed during the current review. The majority of deposit activity originates as ACH deposits from Amazon Marketplace and Walmart Marketplace.

SAR ID# 000012345—John Doe dba XYZ Video

A SAR was filed on our customer, John Doe (DOB: January 01, 0000, SSN 123-45-6789), and his business, XYZ Video, located at 501 W. Ocean Blvd., Long Beach, California for suspicious cash withdrawals totaling $2,295,863.09. The withdrawals were from the customer's personal checking account, #10987654321, and business checking account, #1198765432, between the dates of September 2, 2016 through June 12, 2017. This type of activity is inconsistent with the nature and expected activity of the business (video store) and gave the appearance of possible intent to disguise the flow of funds in a manner consistent with money laundering practices. The cash withdrawals are suspicious since the cash volume is not consistent with expectations based on the business' size and location and there is an absence of legitimate business activity in the accounts. A search using third-party

[8] Planning, collection, analysis, dissemination and feedback form the basis of what is known as the intelligence cycle.

[9] Section 314(b) of the 2001 USA PATRIOT ACT enables cooperative efforts between financial institutions to deter money laundering, https://www.congress.gov/bill/107th-congress/house-bill/3162/text

[10] 31 U.S. Code Section 5318(h)(1) and 31 Code of Federal Regulations Section 1020.210 mandate that financial institutions implement and maintain AML programs to include "ongoing monitoring to identify and report suspicious transactions."

[11] Nick J. Maxwell and David Artingstall, "The Role of Financial Information-Sharing Partnerships," Royal United Services Institute, October 2017, https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwwell_artingstall_web_2.pdf

[12] While personally identifiable information will aide in the review of SAR summary submissions, the sender should adhere to the information sharing protocol of their financial institution.

software specializing in public records noted the business is an extremely small one-room store barely larger than a kiosk in a strip mall and the amount of cash being withdrawn does not make sense. It appears unlikely that a business this size would be able to accumulate over $2 million in third-party checks.

A sample of the suspicious transactions follows:

- On September 2, 2016, $45,000.00 in cash was withdrawn from account #10987654321 at California branch #5678
- On September 21, 2016, $25,000.00 in cash was withdrawn from account #11987654321 at California branch #5678
- On November 4, 2016, $10,000.00 in cash was withdrawn from account #11987654321 at California branch #5678
- On June 9, 2017, $40,000.00 in cash was withdrawn from account #10987654321 at California branch #5678
- On June 12, 2017, $10,000.00 in cash was withdrawn from account #11987654321 at California branch #1234

Both examples expose activity that El Camino Real's intelligence cell would probe further. Each submission contains enough information to quantify the scope of the scheme, potential perpetrators, locus, link to an identified threat sector (respectively, trade fraud and narcotics proceeds) and reasonable suspicion of criminal activity From here, the intelligence cell can further develop the information, possibly request supporting documentation from the bank, analyze the data and refer it to the relevant law enforcement partner via the El Camino Real Switchboard. The receiving agency will decide if further investigation is warranted.

Reveal

Project Reveal is an initiative of El Camino Real promoting the IRS-CI Law Enforcement Assistance Program on identity theft. This program allows state and local law enforcement officials who have evidence of identity theft involving fraudulently filed federal tax returns to obtain consent and disclosure of tax records. State and local law enforcement officials who have evidence of identity theft involving fraudulently filed federal tax returns must contact the identity theft victims to request and secure the victims' consent for disclosure of the tax records. If the victim cannot be located, the IRS can assist in locating taxpayers and soliciting their consent. Victims who opt to participate must complete a special IRS disclosure form (Form 8821-A). State and local law enforcement officers can obtain and return a copy of the Form 8821-A from their local IRS-CI office or El Camino Real. The IRS will process the disclosure forms received and forward the documentation to the law enforcement officer who requested the documents.[13]

Green River

Project Green River is a bulk cash-smuggling initiative. Despite the clever machinations of the criminal class to conceal their tradecraft, cash remains a common and perplexing denominator. There are unlicensed money couriers[14] operating throughout the region and many are delivering drug proceeds to suppliers or businesses that are wittingly or unwittingly participating in trade-based money laundering. Project Green River is designed to develop and pass investigative leads and findings via the El Camino Real Switchboard to law enforcement partners in the affected jurisdictions where the tracing of cash can expose criminal actors and infrastructure.

Maestro

Transnational criminal organizations often utilize sophisticated methods to conceal their activity, their relation to it as well as the placement and layering of their illicit proceeds. The techniques used to conceal and legitimize the proceeds are frequently devised by professionally trained persons engaged in regulated professions such as the law, banking, real estate and finance. Project Maestro aims to target these persons because their corrupt influence can exponentially impact a myriad of criminal schema.

El Camino Real is premised on the expectation that joint engagement by commonly oriented and motivated people will foster cohesion and promote synergy. El Camino Real is a new initiative sponsored by HIFCA to promote broader police-to-police engagement as well as the public-private sector partnerships that holistically is critical to success within the AML sphere. Identifying stakeholders, opening pathways of communication, while being cognizant of defined roles and industry expectations will ultimately enhance access to information, resources and experience as well as safer, integral nation.

Gregory Mandoli, JD, MA, supervisory special agent, Homeland Security Investigations, Los Angeles, CA, USA, gregory.mandoli@dhs.gov

[13] "How IRS Criminal Investigation Partners with Law Enforcement," IRS, https://www.irs.gov/compliance/criminal-investigation/how-irs-criminal-investigation-partners-with-law-enforcement-to-stop-identity-thieves

[14] This is a term of art referencing persons engaged in unreported bulk cash transfers in violation of Title 18 U.S. Code Section 5331. The act is related, but contextually different from violations of Title 18 U.S. Code Section 5330 regarding unlicensed money transmitters, colloquially referred to as informal value transfer systems or Hawalas.

SHALINI PAVITHRAN: THE IMPACT OF MSBS IN MALAYSIA

ACAMS Today had the opportunity to speak with Shalini Pavithran, chief executive officer (CEO) of the Malaysian Association of Money Services Business (MAMSB), about how the money services business (MSB) industry has grown and the unique challenges it presents to the Asia-Pacific region.

As a CEO, Shalini is responsible for the overall management and administration of the association in line with the strategic direction set by the MAMSB Council. She works closely with the Central Bank of Malaysia to promote modernization, enhance professionalism and support the development and growth of the MSB industry. MAMSB and its Group of Compliance Officers' Committee (GOCO) have developed a rigorous mandatory certification and accreditation process for the industry's compliance officers to enhance their competency and to strengthen anti-money laundering/counter-terrorist financing (AML/CTF) compliance across the industry.

In addition, Shalini has extensive experience in the financial sector with about 20 years of banking experience, having served in organizations such as Hong Leong Bank and Alliance Bank. She played a key role in various areas including group and branch operations and management, branch development, banking operations, strategic planning, customer experience management, service quality, business process re-engineering, compliance, risk management, change management, training and development.

ACAMS Today: ***How has the MSB industry evolved in the Asia-Pacific region?***

Shalini Pavithran: In the last 10 years, the MSB industry has changed significantly due to regulatory changes, technological advancements and competition. The stereotypical MSBs of traditional, family-owned businesses that use very basic tools such as the electronic calculator have transformed themselves into modern, well-structured organizations that use the latest technology. MSBs have made huge investments to leverage technology in operations, risk and compliance, brand building, enhancing customer experience and moving toward digitalization of their service. We have seen the digitalization of MSBs taking place in countries such as Australia, New Zealand, Singapore and Malaysia. The regulatory sandboxes introduced by regulators in the region including Malaysia, Singapore, Indonesia, Thailand and Hong Kong have also seen a new generation of MSBs emerging or existing MSBs testing new ideas in a "safe space" without immediately incurring all the normal regulatory consequences.

We have seen significant strides made by the MSB industry over the years with double-digit growth registered in remittances and currency exchange. The cost of money remittances has also fallen with several countries meeting or surpassing the World Bank's target of reducing costs to 5 percent with Malaysia having among the lowest remittance costs in comparison with other markets. In Malaysia, the average remittance cost is well below 3 percent and MSB companies offer some of the most competitive rates for currency exchange in this part of the world.

As MSBs are one of the fastest growing businesses, development in the MSB space is being observed by all parties. In viewing this, MSBs realize that they need to evolve and transform their business to give comfort to their stakeholders.

AT: ***What role has technology played in the modernization of compliance, risk management and training of MSBs?***

SP: The MSBs in the region have been technologically advancing as evidenced by the changing face of MSBs. Recently, digital players have been emerging strong in this region to complement the services of traditional brick-and-mortar players. MSBs in Malaysia are comprised of currency exchange, wholesale currency and remittance companies. Generally, the remittance industry leads the way in leveraging technology but currency exchange is now catching up. In light of the current business realities of intense competition, rising compliance costs and reduced profits, technology has a big part to play to address these concerns and to transform the industry. We have been actively advocating here for technology to be used to drive down compliance costs and challenge stereotypes in the industry. The regulator has also encouraged innovation in our industry as seen with the introduction of the regulatory sandbox and through the issuance of the guideline in November 2017 allowing approved remittance companies to

implement e-know your customer (e-KYC) to enable non face-to-face customer due diligence (CDD) through online or mobile channels.

Our members welcomed this move as they venture into the digitalization of MSB services to meet the changing and rising consumer expectations of the channels they prefer to use. The regulator has also encouraged MSBs to use big data, geospatial analytics and mobile applications to enable effective customer profiling and create bespoke MSB products that are easily accessible to consumers. By finding new and innovative ways to reach out to consumers, the aim is to remove the barriers and migrate more consumers to formal channels. Besides e-KYC, MSBs have been utilizing technology in numerous ways such as customer onboarding, ID verification, sanction and politically exposed person (PEP) screening, transaction monitoring and ongoing risk assessment to name a few. MSBs here have also invested heavily in IT system integration of risk-based approaches and, for our larger industry players, they have taken bold steps to use big data and artificial intelligence for transaction and real time monitoring.

In an effort to make these solutions accessible to all members, we are currently working to introduce an industry platform for sanction and PEP screening as well as transaction monitoring at an affordable cost for our members.

For training, we have organized numerous compliance-training programs for members to attend across the country. However, we also recognize that having an online training platform helps increase training enrollment, reduces the strain on our training resources, provides flexibility to users, provides comprehensive reporting, audit trails and accurate training record keeping, and enables training programs to be dynamic and updated when required. A number of our MSBs have their in-house learning management system and in the coming year, we plan to introduce an industry-wide online training platform to make it affordable for member companies of any size to use the solution, which allows the benefits to be reaped by all our members.

AT: ***How have MSBs adapted their compliance programs to accommodate the new challenges brought about by cryptocurrencies?***

SP: The MSB industry is highly regulated and presently the MSBs are monitoring the developments closely. We are also closely tracking the developments in the region, such as in Japan where regulations on cryptocurrencies have been introduced. We will work with the regulator to adopt any regulations and to adapt the MSBs' compliance programs to address any emerging risks.

AT: ***Tell us about your efforts in building partnerships with local law enforcement and have those partnerships helped foil human trafficking, drug trafficking rings or other types of criminal activity?***

SP: In the last four years, we have been engaging relevant stakeholders including law enforcement agencies such as the police, customs and local authorities to ensure we strengthen safeguards and share information to highlight the issue of illegal remittance and illegal cross-border movement of currencies. While these efforts do take time to bear fruit, we have observed progress being made over the years and we will continue our work to strengthen public-private partnerships in this area.

We are also participating by having key experts and leaders from the industry speak at the Central Bank's Certified Financial Investigator Program, an annual initiative by the Sub-Committee of Capacity Building under the National Coordination Committee to Counter Money Laundering, to enhance the skills and knowledge of financial investigators in fulfilling their task and duties to curb financial crimes. The aim of our participation is to create awareness amongst law enforcement agencies of MSB-specific vulnerabilities to money laundering/terrorist financing (ML/TF) risks, red flags and MSBs' expectation of law enforcement, and to ensure we are aligned in our actions and goals.

AT: ***What are some of the main challenges and/or obstacles MSBs are currently facing in the Asia-Pacific region?***

SP: A changing regulatory landscape in terms of compliance requirements has forced traditional MSBs to rethink their current business models and strategies on how to adapt to these changes. A major challenge for MSBs is also the perception of the industry. Despite all the investments and progress made to improve governance, structure and raise professionalism in the industry and with all the technological advancements, there is still a tendency to use broad strokes and regard MSBs as a high-risk industry.

Due to growing concerns over ML/TF risks, expectations and scrutiny of the MSB industry will continue to rise. In addition, this development has seen MSBs in certain parts of the region be de-risked by banks. The result is adverse social and economic impact to communities and countries that depend on MSBs to receive remittances to raise resources for development. The United Nations Capital Development Fund (UNCDF) reported that in 2017, the formal remittance inflow to Myanmar, Laos, Cambodia and Vietnam stood at $17 billion vs. $6 billion from official development aid to those countries. That number speaks

HAVING MSBS IN THE FINANCIAL SYSTEM AND HAVING VISIBILITY OF ALL TRANSACTIONS AND MOVEMENT OF FUNDS FAR OUTWEIGHS THE BENEFIT OF KEEPING MSBS OUTSIDE THE FINANCIAL SYSTEM

volumes in terms of the impact de-risking MSBs has to the financially vulnerable communities in the region. The de-risking of MSBs also has an unintended consequence of informal systems flourishing with widespread implications for the broader economy leading to a significant increase in unrecorded financial resources.

AT: ***Could you identify some of the areas for improvement to address these unique challenges?***

SP: Addressing the perception issue of MSBs is key and relevant stakeholders should acknowledge the progress made by MSBs. MSBs here have been working to provide strong assurance on the dependability and the integrity of their operations. We have been supporting our industry players' efforts continuously to raise standards of compliance in the industry. Focusing on the initiatives above with the support of the regulator has largely contributed to our industry players having continuous support of relevant banking services for smooth MSB operations. Having MSBs in the financial system and having visibility of all transactions and movement of funds far outweighs the benefit of keeping MSBs outside the financial system.

There is a real need for banks to be aware of the regulatory regime and the progress made by the MSB industry to transform themselves in order for better-informed and more refined risk-assessments of MSBs to be made by banking institutions.

AT: ***What initiatives have you worked on with the Central Bank of Malaysia to strengthen the partnerships and to enhance professionalism between MSBs and banks in Malaysia?***

SP: Our regulator is a key stakeholder of the association and through our collaboration and engagements we have made significant progress to transform the industry. Today, the MSB industry here is among the more developed money services markets in the world and the good standing of the industry has been one of the reasons we have avoided the negative impact from de-risking strategies by banks that have been experienced by other countries.

The association plays a key role in capacity building through its training and education programs for MSB companies that serve to improve performance and compliance, particularly in areas relating to AML/CTF compliance, financial reporting, operational controls and conduct toward consumers. We also play a key advocacy role to raise professional standards and provide an important platform for the regulator and the industry to engage on regulatory, consumer issues and developmental priorities for the industry.

In line with our five-year strategic blueprint (2015-2020), the formation of the GOCO committee and network was a key milestone that has enabled us to roll out various initiatives to set industry standards, and elevate the competence and effectiveness of compliance officers. With the support of GOCO, we collaborated closely with the Central Bank to develop the AML/CTF certification program for MSB compliance officers. This is a compulsory program for all heads of compliance in the industry. This certification program is a four-part series covering the topics of understanding AML/CTF framework, CDD, suspicious transaction reporting and risk-based approach. Thus far, over 5,400 participants attended the AML/CTF certification program and 964 MSB staff have been certified after successfully completing the AML/CTF certification program.

To ensure the certification program is a success and trainers understand the issues faced by MSBs, the trainers selected were heads of compliance within the industry. To equip them with the skills to be competent trainers, they underwent the Certified Training Professionals program by the Finance Accreditation Agency. We currently have 12 certified trainers for the industry and are continuously working to increase the number.

GOCO also supported us in collaborating with the regulator to develop accreditation programs customized for MSBs through the Finance Accreditation Agency and the Department of Skills Development under the Ministry of Human Resources. It is a regulatory requirement for all heads of compliance in the industry to be accredited via any of these accreditation programs or through other reputable programs to ensure compliance officers have the necessary skills and knowledge of regulatory requirements to perform their role effectively.

The GOCO network today has over 1,100 registered compliance officers within the industry, which is a mandatory requirement for every head of compliance of an MSB company to be a member of. Through GOCO, we have established a help desk to support the compliance community in the industry, chat groups for quick dissemination of information, knowledge-sharing sessions and a resource center. We have also organized three regional conferences, with compliance being a key topic, to share best practices and for the industry to be kept abreast of the latest developments and innovations.

The Central Bank continues to engage constructively with the association to develop a modern, dynamic and progressive industry. Through these regular engagements with the Central Bank, we understand the regulatory expectations and receive feedback on areas for improvement in terms of compliance. Based on the feedback received, we enlist the help of GOCO to run compliance workshops targeted at addressing these gaps. This supplements the AML/CTF certification program and compliance officers' accreditation program that we have in place.

MAKING MSB SERVICES MORE AFFORDABLE AND INCLUSIVE WILL CONTINUE TO BE A KEY PRIORITY

We have also customized programs for different groups within the organization to show appreciation of their roles and to help them be equipped with the right skills and knowledge to effectively carry out their roles in mitigating ML/TF risks. We have done this for the following roles: the AML/CTF program for front liners, the AML/CTF program for CEOs and directors, and the CEOs' and directors' education program. We aim to roll out the continuous professional development program this year, and along with all other initiatives in place, we are working toward inculcating a strong compliance culture across the industry.

Furthermore, with the support of the Central Bank, we worked with our counterparts in the banking sector to educate the banking industry on the regulatory regime and the transformation of the MSB industry to strengthen confidence and trust in the MSB industry. MSBs here also frequently hire talents from the banking industry to strengthen governance and raise professional standards. We also partnered with the Compliance Officers' Networking Group for the banking industry and the Asian Institute of Finance in organizing the *9th International Conference on Financial Crime and Terrorism Financing* last year. These types of collaborations will continue as we aim to shape the perception of the industry.

AT: ***In a conference organized by MAMSB last year, you discussed how technology is testing and shaping regulations. How is technology opening the doors for financial inclusion?***

SP: The wider adoption of financial technology to enhance the convenience and efficiency of MSB services is aimed at increasing the use of formal MSB channels and to overcome geographical barriers that deter some segments of the foreign workers especially those in remote areas from using authorized channels.

Making MSB services more affordable and inclusive will continue to be a key priority. Through the Greenback 2.0 Project that we worked on with the Central Bank and the World Bank, we learned that the CDD process in place was a concern and deterred them from formal channels. This is where technology bridges the gap, for example, by allowing migrants to use mobile applications to make it convenient and simple to send money home. There is certainly a greater push toward digitalization of MSB services to reach out to larger segments of customers. The introduction of guidelines allowing e-know your customer (e-KYC) to be used for remittance will only accelerate the digitalization of MSB services here.

We have also been actively working on innovative approaches to public outreach and engagement to migrate consumers to formal channels. In this regard, we have developed our own mobile application, the MSB Advisor, to provide consumers with easy access to price comparisons, locations of authorized currency exchange and remittance service providers, latest developments and tips on currency exchange and remittance, customer reviews and a channel to report illegal MSB activities. This app allows for greater transparency, convenience and enhanced customer engagement.

Another example of how technology is enabling financial inclusion is through the UNCDF Shift Challenge Fund, which encourages innovative solutions to link remittances as a catalyst for financial inclusion and women's economic empowerment. Some of the successful innovative solutions under the Challenge Fund that used technology were a blockchain-based international remittance transfer mobile app, an open remittance aggregator platform linking local receiving partners with global sending partners and a mobile phone-based e-wallet service providing international remittances.

AT: ***What would be your advice to MSBs who face challenges in getting banking services?***

SP: The landscape and regulations of MSBs have been changing in the past five years. MSBs must adapt to the new norms and work toward meeting these regulatory expectations by investing in talent, systems, enhancing governance structures and organizational setup and leverage on technology. Through these efforts aimed at improving transparency, strengthening safeguards, and raising compliance and professional standards, we will be able to improve perception of the industry.

MSBs can also come together to collectively work on strengthening regulatory compliance to provide strong assurance on the integrity of their operations. Through collaboration toward common goals, industry players may come together to build shared infrastructures or platforms to facilitate the exchange of information or share common utilities for the purpose of raising compliance standards and strengthening safeguards to prevent MSBs from being used to facilitate criminal activity.

Interviewed by: Hue Dang, CAMS-Audit, head of Asia, ACAMS, Hong Kong, hdang@acams.org

Life-changing suits:
Befitting occupations

From belt keepers to gatekeepers, the transition from the public to the private sector may seem like a natural fit. However, how does law enforcement experience measure up when compared to the fierce competition in the anti-money laundering (AML) industry? Are the knowledge, skills and abilities of a law enforcement applicant easily transferable to a position within the Bank Secrecy Act/anti-money laundering (BSA/AML) field? For that matter, what makes a law enforcement applicant best suited for change?

From officer to office

The shift from law enforcement to the private sector may seem like a reward for years of public service, but it is a decision that must be assessed against the realities of the "corporate life." Budget cuts vs. bonuses and financial stability vs. considerable salary are just a few things for law enforcement officers to consider before retiring the lifestyle that is the product of their career. With that in mind, it is necessary to not only mentally prepare for these changes but also to learn how to best capture the career experiences that match the desired qualifications of a hiring firm.

The most important question for hiring firms to ask and for law enforcement to answer is "Why?" The answer to the why question has an impact on your job search experience and drive. Why are you, the applicant, leaving law enforcement and applying for in-house roles? Why did you originally join law enforcement? Why do you believe leaving law enforcement is the best move now? Why is banking and/or

consulting better than the job you have now? How applicants answer these questions will give substantial insight into his/her own driving motivation. Discovering the factors behind your own decision-making process can customize your industry and job search. However, during this journey of self-discovery, it is essential to remember that while the responses may be sincere, it is vital to "dress to impress" the answers. Let us analyze legitimate retirement reasons, but focus on the ornamentation:

- "Because I am retiring"
  - — This is a simple, honest and practical answer. However, hiring managers may doubt your dedication and work ethic after paying your dues and thus make you unfit for the position. It is important to clarify that you are not ready to retire but rather ready to transition your crime-fighting efforts to the private sector. Words matter.
- "Because I want a more flexible schedule"
  - — Although a law enforcement officer may have been classified as "essential" and holidays were nothing more than figments of the imagination, this phrasing could be interpreted by the hiring manager as being a clock-watcher or even indicative of laziness. Practically speaking, while the shift may not wax and wane, the hours remain long and demanding.
- "Because the grass is greener"
  - — A better job? A well-run administration? There are misconceptions about all career fields and it is important to remember politics exist in all organizations and an applicant must be prepared to demonstrate his/her merit coupled with integrity and savviness. In an environment where an annual increase is not guaranteed, ambitions, jealousies and competition are driving factors that must be met with the character expected of a professional law enforcement officer.

DISCOVERING THE FACTORS BEHIND YOUR OWN DECISION-MAKING PROCESS CAN CUSTOMIZE YOUR INDUSTRY AND JOB SEARCH

All dressed up, but where to go?

If expectations are not "sized," this can lead to a different type of law enforcement apprehension; for example, support function angst. What positions

are best suited for a law enforcement applicant to pursue? As the transition becomes reality, applicants must begin by first weighing permanent/full-time roles against contract/consulting roles. Once an applicant realizes their personal goals, he/she can determine if a temporary or long-term position is in line with their expectations.

Fortunately, a law enforcement background is the "cut above" experience that is in demand in all industries. In financial services, though, former law enforcement officers fit well into specific AML and compliance verticals. However, to be clear, qualified and confident law enforcement applicants can get a job in any vertical or department of a financial services firm's compliance program. Some natural fits include:

1. Financial intelligence units (FIU) or transaction monitoring and investigations (TMI): The backbone of a real-time AML and financial security program, FIUs and TMIs help the firm decide whether to work with current and potential clients. They conduct enhanced due diligence on accounts, monitor flagged activity, investigate vetted suspicious activity and begin, what you would consider, the internal version of an official law enforcement investigation.
2. Fraud: Fraud, compliance and BSA/AML are all part of the same mission, but have different arrangements at different institutions. Fraud departments are a great starting point for post-law enforcement, white-collar professionals. Bigger financial institutions that have retail products (retail and consumer banks, retail insurers, fintech firms that provide taxing services [seriously!]) all need fraud investigators for internal employees and external customers.
3. Management consulting: Management consulting gives you the chance to be employed by one company, but travel and work on many different projects with multiple clients. Former examiners and law enforcement professionals have created many boutique and large management-consulting firms.
4. Cybersecurity: Cybersecurity is important to nations and corporations alike. Law enforcement at all governmental levels should consider taking on cybercrime assignments, if possible. Management consulting firms are building out their cybersecurity practice areas too.
5. Physical security: Physical security is a complicated matter when working with multiple locations and the always-varying number of people in any given spot. Law enforcement makes great candidates for physical security roles at banks, real estate management companies and amusement parks (i.e., Disney World).

There is no need to typecast an applicant into one corporate profile. It is also important to investigate the positions that may not have originally been a good fit for a law enforcement skillset and personality. Thus, look at all types of industries.

Where do you want to be when you go into retirement? Ask all your former law enforcement colleagues who went in-house how they are doing. Who is genuinely happy in their new role? You just might be suitable for that same job.

From capturing lowlifes to highlights

With the end of duty begins the concerted effort to underscore the experiences that came with a career in law enforcement. Choosing the content to bullet point in a resume requires a targeted approach to reviewing one's career highlights. An expert score at the firearms range is not an expertise necessarily needed to qualify as a Bank Secrecy Act officer. The natural inclination for a law enforcement officer is to emphasize arrests, successful prosecutions and assignments. What in a law enforcement officer's past should be featured when striving for a future in the BSA/AML field?

While there are no standard templates, there are best practices that provide the guidance necessary to create a "just" resume. Recruiters who specialize in addressing the needs of the private sector by promoting the best of the public sector have shared their successes in order to help law enforcement tailor their curriculum vitae.

Style

Hiring managers and recruiters always want to see an aesthetically pleasing resume. "Good-looking" resumes with substance are hard to pass up. You can use professional resume builders or copy the formatting (not the content) of resumes you like online. Make sure you have multiple people review it. However, be very wary of where and to whom you send your resume. Vet potential recruiters before blindly sending your resume and keep track of how many times you email it. You do not know how many subsequent "forwards" there are. Below are a few of the pertinent recommendations:

- Research your favorite style, template and format that you can copy, enhance and tailor to your own preference and image. Do not rely solely on Microsoft Word or other software resume templates. You should send out resumes that not only proudly summarize your background, but also make you proud of their style. It is important to remember that recruiters or hiring managers' first judgment of who you are is based on the way your resume looks.
- Make sure the structure is clear and consistent. In general, resumes layer information from the big picture to the small details. For instance, we start with our name and end with the software we know best. In addition, within each job we have held, we mention the name of the employer, the years of employment, a description of the employer (maybe), and then a summary of both tactical daily responsibilities and our success stories. Make sure—and this cannot be emphasized enough—that all fonts, sizes, formatting, margins and alignments are 100 percent consistent. Do not fluctuate from formatting consistency even once because discrepancies are relatively easy to spot, especially when you are in the business of looking at them. Moreover, it could create a horn effect (opposite of halo effect) bias from the start.[1]

Hiring managers and recruiters—alike—could believe you are not detail-oriented, do not care enough to edit your resume diligently or are naturally sloppy. Mitigate all chances of being at a disadvantage even before walking through the door for an interview. This is a common circumstance with former law enforcement. Oftentimes, resumes with grammar mistakes or poor style are sent relying on the applicant's reputation rather than what is reflected on paper. Strong writing skills are in demand more than ever.

Content

In place of an objective, include a summary section. Summaries are made up of bullet points of your quantitative and qualitative skills. This is a good section for you to concentrate on buzzwords, such as "analytical skills" or "strong leadership," so that you appear in recruiters' searches. Recruiters use applicant-tracking systems (ATS) to search for candidates' resumes using buzzwords they find on job descriptions, because recruiters, like law enforcement, can have limited time. As a result, you want your resume front and center for roles that pertain to your skillset and background. Lastly, the "one-page resume" is a myth. If you just graduated college or graduate school, you will not have much experience to present, so keep it to one page (and write strong cover letters). Nevertheless, if you have enough content to fill up most of a second page, then go for it. However, this content has to be as important as the information provided on the first page. In addition, if you have a two-page resume, it is suggested to add your educational background information on the second page. This will make any recruiter and talent specialist turn the page. Finally, consider adding the "prized" features. Below are some noteworthy accomplishments that should be highlighted in a resume:

> STYLING A LAW ENFORCEMENT OFFICER'S RESUME THAT GARNERS THE INTEREST OF AN EMPLOYER BEGINS WITH THE MENTAL READINESS OF THE APPLICANT

- Emphasize the extras:
  - — Any and all promotions, such as officer to detective
  - — Both remediation and prevention:
    - What did you discover and fix after the fact?
    - What, from experience, wherewithal and good judgment, did you help prevent?
  - — Investigations, experience and participation
    - To what extent were you involved: participant, team leader, commanding officer, etc.?
    - Successfully being a member of teams and how you added leadership to them
    - The degree of sensitivity, complexity and confidentiality of work
  - — Communication skills with the chain of command, across different jurisdictions and between departments
  - — Formal and informal training you had from being part of special committees, teams or investigations
  - — The positive effect you had on your colleagues. Were you tasked with formally or informally training others?

Designing the cover letter

Like the resume, figure out what formatting fits who you are best. Choose your own style while maintaining the required professionalism.

In addition, have distinct paragraphs, so that each paragraph has a function and purpose. You should have a general cover letter that acts as a template. However, each cover letter you submit has to be tailored to the job you are applying to. For instance, a general cover letter could look like this:

- *Introduction:* Who are you as a person? What sworn position is held and with what agency?
- *Second paragraph:* Describe what you learned in law enforcement and your proud moments.
- *Third paragraph:* Provide a more detailed synopsis of your skillset and life lessons that pertain to that particular role (this will be the most edited paragraph).
- *Conclusion:* Write a wrap-up of who you are, what you have done, what you have learned and most importantly, what you want to do next and why this particular role appeals to you.

Styling a law enforcement officer's resume that garners the interest of an employer begins with the mental readiness of the applicant. Only when a contender has accepted they are no longer serving a process but processing service requests will he/she be a viable candidate. Thus, make sure to accentuate on a resume both the desk-oriented duties (writing, formal presentations, trainings attended and certified, strong communication experience across different levels of management, etc.) and successful involvement in complicated investigations. Having a polished resume is just the beginning. In order to impress at the interview, get ready to roll up your sleeves.

Stacey Ivie, M.Ed., task force officer, Washington Baltimore HIDTA, Northern Virginia Financial Initiative (NVFI), Annandale, VA, USA, sivie@wb.hidta.org

Sanjeev Menon, ACAMS Career Guidance columnist, compliance, legal and privacy senior practice area manager, Infinity Consulting Solutions, Inc., New York, NY, USA, smenon@infinity-cs.com

[1] The halo effect and horn effect are both biases we all succumb to. The halo effect occurs when you have a positive view of someone based on an action (quality, characteristic, value, etc.) that skews your judgement. The horn effect occurs when you have a negative opinion that affects your assessment and causes you to have a negative impression of all subsequent interactions.

A great gangster story with a lesson on leadership

Good stories usually have five key elements: a likable protagonist that selflessly rises to the occasion; a malevolent antagonist seeking to oppress others; an impactful event that sets the characters in motion; a conflict that creates seemingly insurmountable challenges; and a climactic resolution so pleasing it serves to inspire us. This is the stuff of blockbuster movies. When all five elements can be encapsulated in the events of a real person's life, then you have a really great story. Such is the story of Elmer Lincoln Irey.

Irey was the first chief of the Intelligence Unit (which was later changed to IRS Criminal Investigation), a law enforcement branch of the U.S. Department of the Treasury created in 1919 to attack the growing problem of tax evasion occurring after WW1. Income tax rates had been significantly hiked to help pay for the mounting debts incurred during the Great War. But there were those of an unpatriotic ilk that had no interest in handing over larger portions of their income. It was Irey's job to establish and oversee a band of investigators to tediously follow the money and build criminal tax evasion cases on the nation's biggest tax dodgers. Irey's unit was commonly referred to as the "T-MEN" to differentiate them from the famed "G-MEN" of the Federal Bureau of Investigation.

On the surface, the work of Irey's Intelligence Unit may sound a bit mundane—laboriously combing through ledgers, bank records and receipts—but that was not how Congressman John Cochran saw it. In his speech to congressional colleagues in 1940, Cochran told them, "If the true story of his [Elmer's] activities could be put in book form it would be classed as one of the best sellers in the United States. There is not a section of the country they have not invaded."[1] *Life* magazine amplified the Congressmen's assessment, proclaiming that Irey's T-MEN "involved themselves in some of the greatest cops-and-robbers escapades in history."[2]

The antagonists

The evil villains in Irey's story are gangsters. Not run of the mill gangsters but T-Rex-sized violent crime bosses of comic book proportions that flourished during Prohibition era. Their vast criminal enterprises earned millions of dollars through the sale of alcohol, prostitution, illegal gambling and commerce extortion rackets. If you wanted to do business, well…you better pay them. By the mid-1920s, nearly every major city had a kingpin crime overlord.

Yes, violence and intimidation played a role, but what really empowered the gangsters was a culture of corruption that permeated in the 1920s. When you line the pockets of councilmen, judges, police officials, prohibition agents and governors, you become untouchable. Because of corruption, the honest cops were hamstrung in dealing with the organized crime wave. Famed journalist and author, Marquis Childs, explained the Gotham-like atmosphere of the time: "In city after city, in communities large and small, crime was licensed, subsidized. Decent people despaired." Along with the gangsters, corrupt officials were also the evil villains.

The impactful event

What set Irey in motion with his antagonists was the St. Valentine's Day Massacre. On Valentine's Day 1929, seven people were lined up against a wall in a Chicago warehouse and gunned downed execution style with submachine guns. The reigning

[1] Proceedings and Debates of the 76 Congress, Third Session.

[2] *Life*, September 2, 1946, 46-47.

Elmer Irey in his office overseeing the many high profile investigations under his direction.

theory was that the infamous kingpin, Al Capone, ordered some of his 1,000-plus army of gangsters to make the hit. The victims were members of a rival criminal enterprise known as the Northside Gang led by the kingpin George "Bugs" Moran. Capone was bent on violently taking over Moran's territory. To Capone, it was just business.

The St. Valentine's Day Massacre received mass media attention and ignited a public outrage toward the violence and corruption engulfing the nation. In response to outcries, President Herbert Hoover made it his priority to rid the country of crime bosses and at the top of his list was the infamous Capone.

At the time, there were few federal laws specifically designed to combat organized crime. Even though the Bureau of Prohibition made thousands of arrests, they had been frustratingly ineffective in roping in the ringleaders. Out of desperation, President Hoover ordered Irey to get Capone. As *Life* magazine put it, "When gangsters and crooked politicians defied the local laws, the T-MEN nabbed their men for the federal crime of tax evasion."[3]

Seemingly insurmountable challenges

The task at hand for Irey was definitely not a simple and safe walk in the park. When Capone learned that the T-MEN were on his case, witnesses mysteriously turned up missing or dead. It was a dangerous assignment and Irey regularly received death threats. Irey was unfazed by the threats on his own life but obsessively worried about the well-being of his agents.

Using tax laws to bring down crime overlords was a novel approach. Like Lewis and Clark, Irey was headed down uncharted waters. Capone paid cash for everything, kept no books and records in his name and had extremely loyal minions secretly handling his financial affairs. Capone claimed he was a professional gambler on a losing streak. On paper, Capone appeared to be flat broke.

Going after Capone's money trail would undoubted lead to the exposure of corrupt officials. Capone paid about 20 cents on every dollar he earned to graft. Like other major city kingpins, Capone made generous political cash contributions to politicians. Irey could have stepped on big, influential toes, the toes of those that could have toppled his career or cut funding for his unit. The astute Director of the FBI, J. Edgar Hoover, acknowledged the hazards of such investigations and avoided organized crime cases altogether.

To build cases on entrenched crime bosses you first need intelligence on the inner-workings of the organization and that meant long-term undercover operations. Only the most experienced undercover agents would stand a chance blending in with hardened gangsters. At the time, Hoover would not take the risk of letting his agents do such undercover work for fear they would succumb to the vices of the gangsters. However, Irey's top undercover agent infiltrated the Capone organization and lived with Capone's gang for over a year without compromise.

Even if Irey's team put together a prosecutable case there was still the demoralizing realization Capone would bribe and intimidate the jury (which Capone later attempted). There was also the risk of an agent capitulating to a bribe. A corrupt prohibition agent could earn thousands of dollars by merely letting a truckload of whiskey pass by. Capone tried to bribe Irey with a million dollars, which he summarily declined.

In order to have a fighting chance, Irey needed a top-notch team of seasoned criminal investigators skilled at following the money, unencumbered by fear with unassailable integrity and honestly. The team would have to be so steadfastly loyal to the mission they would be willing to work

[3] Ibid.

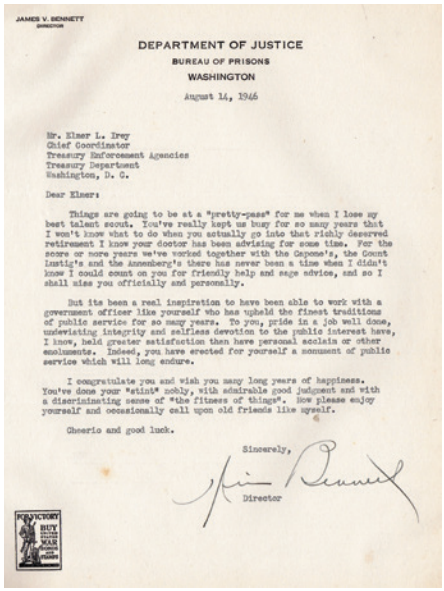
excruciatingly long hours for months on end under dangerous conditions, ever motivated to follow the slightest financial lead.

The climactic battles and victories

On October 18, 1931, the front headlines of all major newspapers reported the conviction of Capone on tax evasion, making Irey and his T-MEN instant folk heroes. The conviction was such a motivating factor that lines of mobsters formed at IRS offices to file tax returns. Tax collections in the Chicago area more than doubled.

Without a rest, Irey and his T-MEN went to New York and took on infamous gangsters Waxey Gordon, Dutch Schultz and Capone's mentor, Johnny Torrio. They then applied their investigative prowess on the Huey Long Gang of Louisiana; Kansas City's political boss Tom Pendergast; and Atlantic City's Lord of Atlantic City, Nucky Johnson, who was the inspiration for HBO's *Boardwalk Empire*. Irey and his T-MEN were invading so many crime bosses and corrupt officials they earned the nickname *The Giant Killers*. The T-MEN even saved Hollywood by stopping Capone's remaining gang, led by ruthless killer Frank Nitti, in their tracks from controlling the motion picture industry.

Elmer Irey conferring with a high level treasury official.



JAMES V. BENNETT
DIRECTOR

DEPARTMENT OF JUSTICE
BUREAU OF PRISONS
WASHINGTON

August 14, 1946

Mr. Elmer L. Irey
Chief Coordinator
Treasury Enforcement Agencies
Treasury Department
Washington, D. C.

Dear Elmer:

Things are going to be at a "pretty-pass" for me when I lose my best talent scout. You've really kept us busy for so many years that I won't know what to do when you actually go into that richly deserved retirement I know your doctor has been advising for some time. For the score or more years we've worked together with the Capone's, the Count Lustig's and the Annenberg's there has never been a time when I didn't know I could count on you for friendly help and sage advice, and so I shall miss you officially and personally.

But its been a real inspiration to have been able to work with a government officer like yourself who has upheld the finest traditions of public service for so many years. To you, pride in a job well done, unbewitching integrity and selfless devotion to the public interest have, I know, held greater satisfaction than have personal acclaim or other emoluments. Indeed, you have erected for yourself a monument of public service which will long endure.

I congratulate you and wish you many long years of happiness. You've done your "stint" nobly, with admirable good judgment and with a discriminating sense of "the fitness of things". Now please enjoy yourself and occasionally call upon old friends like myself.

Cheerio and good luck.

Sincerely,

Director

VICTORY BUY UNITED STATES WAR SAVINGS BONDS

In 1942, when the nation was heavily reliant on income tax collections to fund WW2, President Franklin Roosevelt (FDR) sent Irey a personal letter of appreciation on White House stationary that stated, "Over the years the Intelligence Unit has become not only a shiny mark of incorruptibility but also A-1 Service."[5]

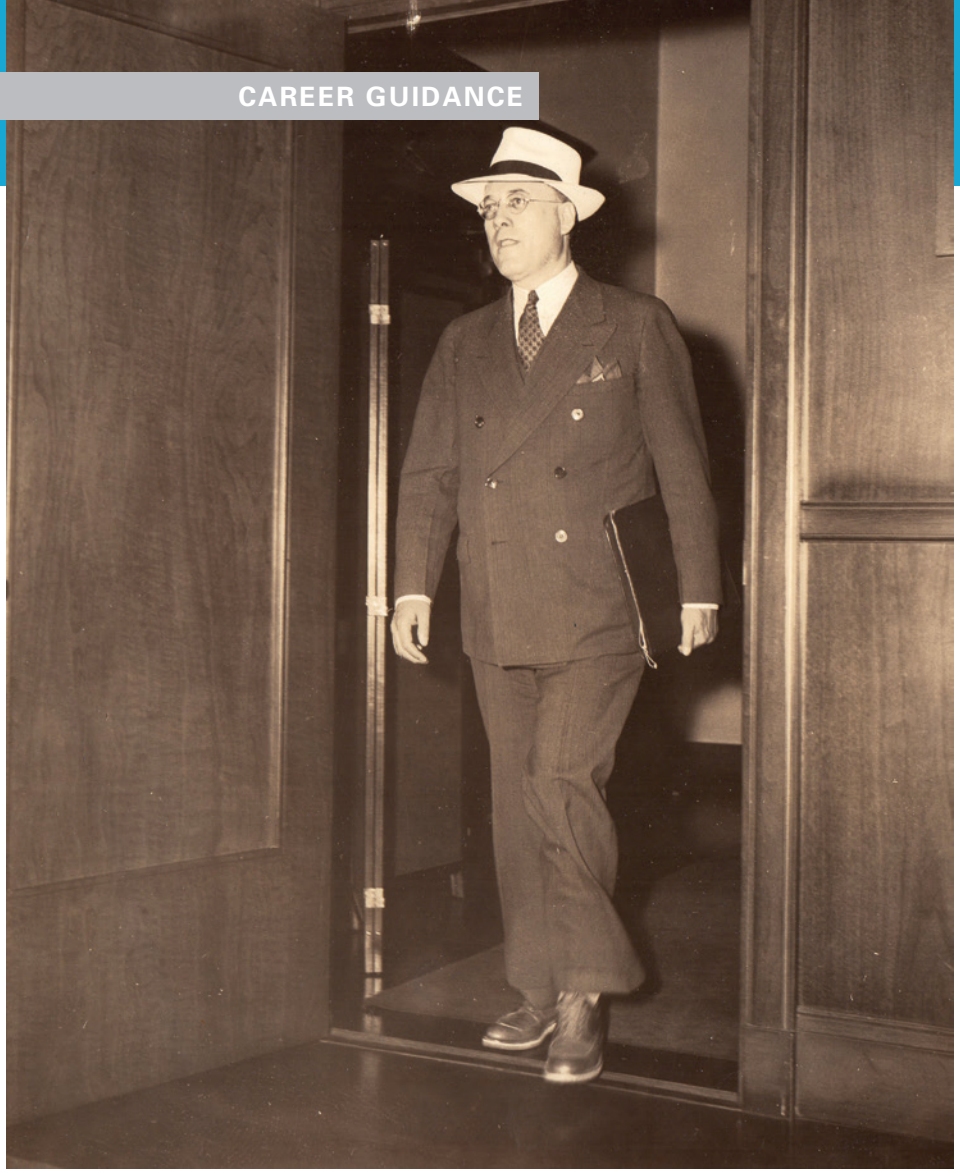
In 1945, Westbrook Pegler, a popular conservative columnist who wrote extensively on professional sports scandals was asked by the baseball industry what he thought of Irey as a candidate for the new baseball administrator. Pegler responded by saying he did not know what Irey knew about baseball but if Irey was not honest, "there weren't no God."[6]

Irey served in a senior law enforcement position from 1919 to 1946, retiring due to a failing heart. Upon his retirement, Irey received numerous letters of praise from

[4] Letter to Elmer Irey from James Bennett, dated August 1946, original in possession of Mob Museum.

[5] Letter to Elmer Irey from President Franklin Roosevelt dated March 1942, original in possession of Mob Museum.

[6] Letter to Elmer Irey from Westbrook Pegler dated August 28, 1946, original in possession of Mob Museum.



Elmer Irey attending meetings to coordinate the various treasury enforcement agencies.

well-wishers, colleagues and former staff. The Chairman of the Import Export Bank wrote Irey, "Your record as a public servant cannot be exceeded. It is without a blemish, and there has never been a scintilla of criticism directed against you notwithstanding the thousands of cases investigated and prosecuted under your personal direction."

Homer Cummings, the U.S. Attorney General under FDR, wrote to Irey: "As you are aware, I have been familiar with your public service over a long period of time, and in my judgment no one has rendered more distinguished public service than you have." Interestingly, Cummings, as the attorney general, was Hoover's boss and an early supporter of the famous FBI director.

Marquis Child—the first to win a Pulitzer Prize for distinguished commentary—wrote Irey, "Your long and distinguished service is an occasion for pride not alone to your family and wide circle of friends but to everyone who believes in effective, honest government."

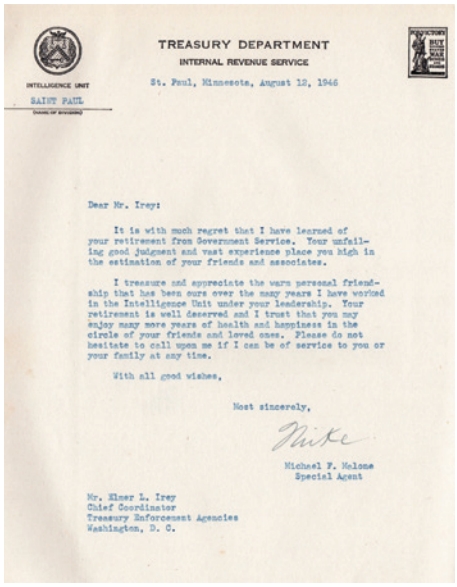
Arguably, Irey was one of the most respected and accomplished law enforcement leaders in the history of the United States. So how did he do it?

The power of character

In his letter to Irey, U.S. Attorney and later Federal Judge William T. McCarthy eloquently described what enabled Irey's success. "The worth-while satisfaction, Elmer, that one can get out of public service can only be measured by the attributes of honesty, integrity, forbearance, sound judgment, patience, and charity, the latter attribute not misapplied, but exercised in conformity with the standards of simple justice. These attributes are a part of the Golden Treasury of life and you have been blessed by having them as your treasured possessions." Simply put, McCarthy was telling Irey it was his character.

Alf Oftedal—the agent that led the fight to save Hollywood—said in his letter to Irey, "Emerson has observed that men of character are the conscience of the society to which they belong. How true this is, as evidenced by your outstanding influence among special agents. They, quite naturally, considered it a great honor to have been selected for important duties under your direction."[7]

Those who choose to lead with honesty, integrity, forbearance, sound judgment, patience, charity and "simple justice" are leaders of character. They lead by example and by doing so, foster a culture of



TREASURY DEPARTMENT
INTERNAL REVENUE SERVICE
INTELLIGENCE UNIT
SAINT PAUL
St. Paul, Minnesota, August 12, 1946

Dear Mr. Irey:

It is with much regret that I have learned of your retirement from Government Service. Your unfailing good judgment and vast experience place you high in the estimation of your friends and associates.

I treasure and appreciate the warm personal friendship that has been ours over the many years I have worked in the Intelligence Unit under your leadership. Your retirement is well deserved and I trust that you may enjoy many more years of health and happiness in the circle of your friends and loved ones. Please do not hesitate to call upon me if I can be of service to you or your family at any time.

With all good wishes,

Most sincerely,

Michael F. Malone
Special Agent

Mr. Elmer L. Irey
Chief Coordinator
Treasury Enforcement Agencies
Washington, D. C.

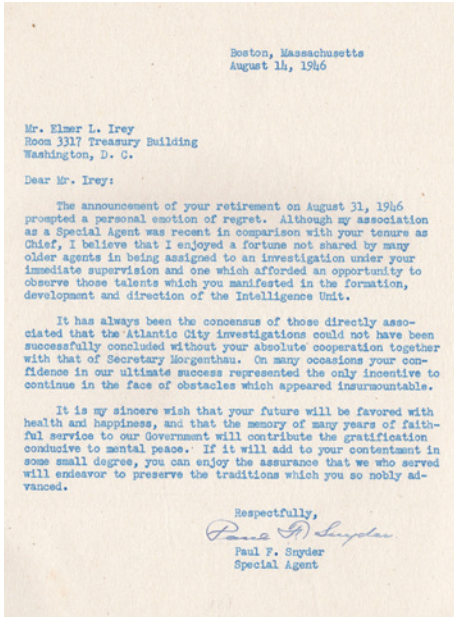
[7] Letter to Elmer Irey from Alf Otfeda dated August 1946, original in possession of Mob Museum.

character that inspires others to mirror their attributes. This is how Irey made his unit a "shiny mark of incorruptibility."

Agent Tom Henry said in his letter to Irey, "Above all you have shown every man who has worked for or with you that true value of integrity, loyalty and sound common sense."[8] Agent E.C. Palmer wrote, "The Unit carries and will jealously safeguard the enduring stamp of your character and integrity."[9]

Leaders of character work toward a higher purpose than themselves. They strive to be selfless, humble and never self-aggrandizing. Stephen Spingarn—the assistant general counsel for the U.S. Treasury who also served as special counsel to FDR and President Truman—wrote Irey, "I have particularly admired the selflessness with which you have carried on your work, avoiding the notable opportunities which it might have afforded another sort of man for self-glorification, and concentrating only on doing the job."[10] Reading between the lines, the "another sort of man" Springarn alluded to was Hoover. When Springarn was the assistant attorney general, he worked closely with Hoover. By Hoover's edict, every FBI press release only bared the name "J Edgar Hoover" and the FBI director reveled in the spotlight.

Leaders of character are not obstinate taskmasters. They understand the value of encouraging others to achieve "A-1 service." Agent Muray Dengler said to Irey, "You drove your teams with an easy rein which gave them more confidence in themselves and made all of them give their best to you."[11] Paul Synder—one of the agents that brought down crime boss Nucky Johnson—told Irey, "On many occasions your confidence in our ultimate success represented the only incentive to continue in the face of obstacles which appeared insurmountable."[12]



Boston, Massachusetts
August 14, 1946

Mr. Elmer L. Irey
Room 3317 Treasury Building
Washington, D. C.

Dear Mr. Irey:

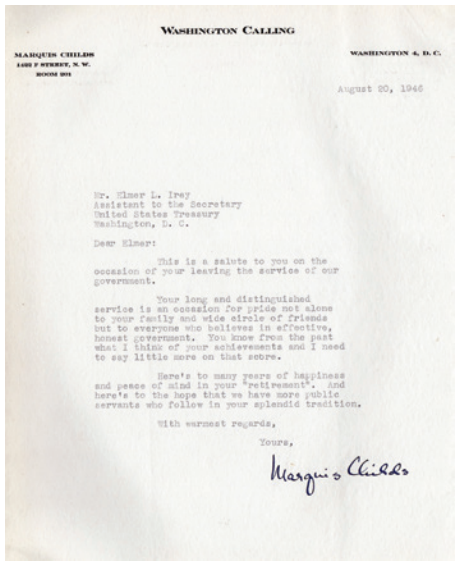
The announcement of your retirement on August 31, 1946 prompted a personal emotion of regret. Although my association as a Special Agent was recent in comparison with your tenure as Chief, I believe that I enjoyed a fortune not shared by many older agents in being assigned to an investigation under your immediate supervision and one which afforded an opportunity to observe those talents which you manifested in the formation, development and direction of the Intelligence Unit.

It has always been the concensus of those directly associated that the Atlantic City investigations could not have been successfully concluded without your absolute cooperation together with that of Secretary Morgenthau. On many occasions your confidence in our ultimate success represented the only incentive to continue in the face of obstacles which appeared insurmountable.

It is my sincere wish that your future will be favored with health and happiness, and that the memory of many years of faithful service to our Government will contribute the gratification conducive to mental peace. If it will add to your contentment in some small degree, you can enjoy the assurance that we who served will endeavor to preserve the traditions which you so nobly advanced.

Respectfully,

Paul F. Snyder
Special Agent



WASHINGTON CALLING

MARQUIS CHILDS
1400 F STREET, N.W.
ROOM 901

WASHINGTON 4, D. C.

August 20, 1946

Mr. Elmer L. Irey
Assistant to the Secretary
United States Treasury
Washington, D. C.

Dear Elmer:

This is a salute to you on the occasion of your leaving the service of our government.

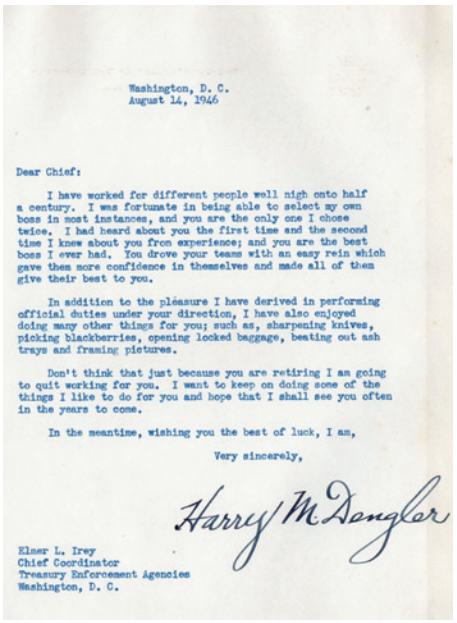
Your long and distinguished service is an occasion for pride not alone to your family and wide circle of friends but to everyone who believes in effective, honest government. You know from the past what I think of your achievements and I need to say little more on that score.

Here's to many years of happiness and peace of mind in your "retirement". And here's to the hope that we have more public servants who follow in your splendid tradition.

With warmest regards,

Yours,

Marquis Childs



Washington, D. C.
August 14, 1946

Dear Chief:

I have worked for different people well nigh onto half a century. I was fortunate in being able to select my own boss in most instances, and you are the only one I chose twice. I had heard about you the first time and the second time I knew about you from experience; and you are the best boss I ever had. You drove your teams with an easy rein which gave them more confidence in themselves and made all of them give their best to you.

In addition to the pleasure I have derived in performing official duties under your direction, I have also enjoyed doing many other things for you; such as, sharpening knives, picking blackberries, opening locked baggage, beating out ash trays and framing pictures.

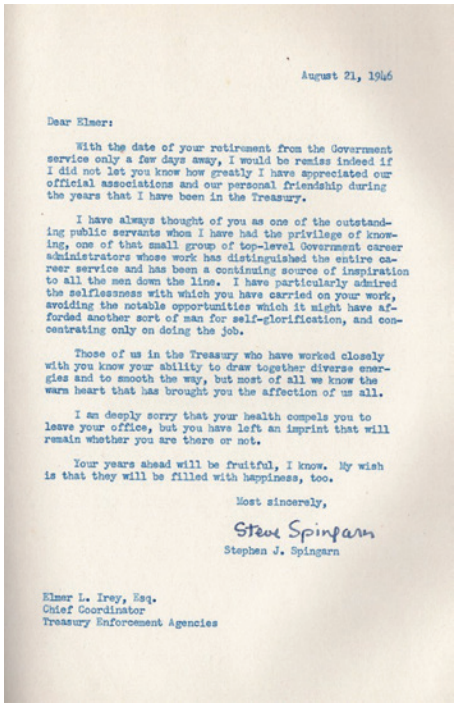
Don't think that just because you are retiring I am going to quit working for you. I want to keep on doing some of the things I like to do for you and hope that I shall see you often in the years to come.

In the meantime, wishing you the best of luck, I am,

Very sincerely,

Harry M. Dengler

Elmer L. Irey
Chief Coordinator
Treasury Enforcement Agencies
Washington, D. C.



August 21, 1946

Dear Elmer:

With the date of your retirement from the Government service only a few days away, I would be remiss indeed if I did not let you know how greatly I have appreciated our official associations and our personal friendship during the years that I have been in the Treasury.

I have always thought of you as one of the outstanding public servants whom I have had the privilege of knowing, one of that small group of top-level Government career administrators whose work has distinguished the entire career service and has been a continuing source of inspiration to all the men down the line. I have particularly admired the selflessness with which you have carried on your work, avoiding the notable opportunities which it might have afforded another sort of man for self-glorification, and concentrating only on doing the job.

Those of us in the Treasury who have worked closely with you know your ability to draw together diverse energies and to smooth the way, but most of all we know the warm heart that has brought you the affection of us all.

I am deeply sorry that your health compels you to leave your office, but you have left an imprint that will remain whether you are there or not.

Your years ahead will be fruitful, I know. My wish is that they will be filled with happiness, too.

Most sincerely,

Steve Spingarn
Stephen J. Spingarn

Elmer L. Irey, Esq.
Chief Coordinator
Treasury Enforcement Agencies

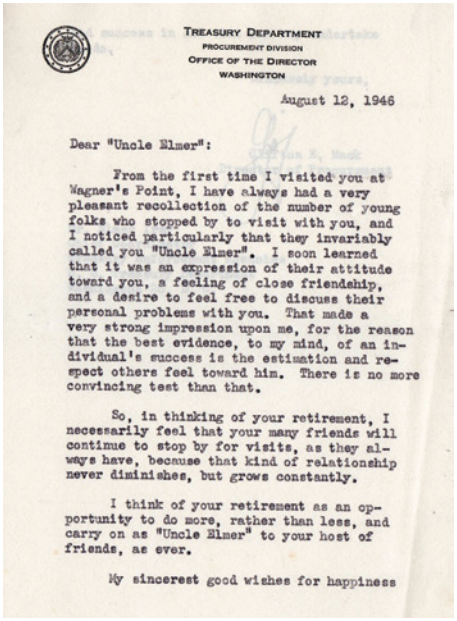
[8] Letter to Elmer Irey from Tom Henry dated August 1946, original in possession of Mob Museum.

[9] Letter to Elmer Irey from Special Agent in Charge E.C Palmer dated August 15, 1946, original in possession of Mob Museum.

[10] Letter to Elmer Irey from Stephen J. Spingarn dated August 21, 1946, original in possession of Mob Museum.

[11] Letter to Elmer Irey from Muray M. Dengler dated August 1946, original in possession of Mob Museum.

[12] Letter to Elmer Irey from Paul Snyder dated August 14, 1946, original in possession of Mob Museum.



TREASURY DEPARTMENT
PROCUREMENT DIVISION
OFFICE OF THE DIRECTOR
WASHINGTON

August 12, 1946

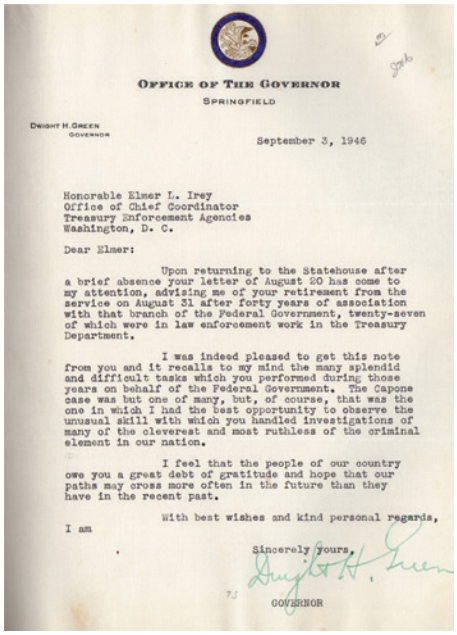
Dear "Uncle Elmer":

From the first time I visited you at Wagner's Point, I have always had a very pleasant recollection of the number of young folks who stopped by to visit with you, and I noticed particularly that they invariably called you "Uncle Elmer". I soon learned that it was an expression of their attitude toward you, a feeling of close friendship, and a desire to feel free to discuss their personal problems with you. That made a very strong impression upon me, for the reason that the best evidence, to my mind, of an individual's success is the estimation and respect others feel toward him. There is no more convincing test than that.

So, in thinking of your retirement, I necessarily feel that your many friends will continue to stop by for visits, as they always have, because that kind of relationship never diminishes, but grows constantly.

I think of your retirement as an opportunity to do more, rather than less, and carry on as "Uncle Elmer" to your host of friends, as ever.

My sincerest good wishes for happiness



OFFICE OF THE GOVERNOR
SPRINGFIELD

DWIGHT H. GREEN
GOVERNOR

September 3, 1946

Honorable Elmer L. Irey
Office of Chief Coordinator
Treasury Enforcement Agencies
Washington, D. C.

Dear Elmer:

Upon returning to the Statehouse after a brief absence your letter of August 20 has come to my attention, advising me of your retirement from the service on August 31 after forty years of association with that branch of the Federal Government, twenty-seven of which were in law enforcement work in the Treasury Department.

I was indeed pleased to get this note from you and it recalls to my mind the many splendid and difficult tasks which you performed during those years on behalf of the Federal Government. The Capone case was but one of many, but, of course, that was the one in which I had the best opportunity to observe the unusual skill with which you handled investigations of many of the cleverest and most ruthless of the criminal element in our nation.

I feel that the people of our country owe you a great debt of gratitude and hope that our paths may cross more often in the future than they have in the recent past.

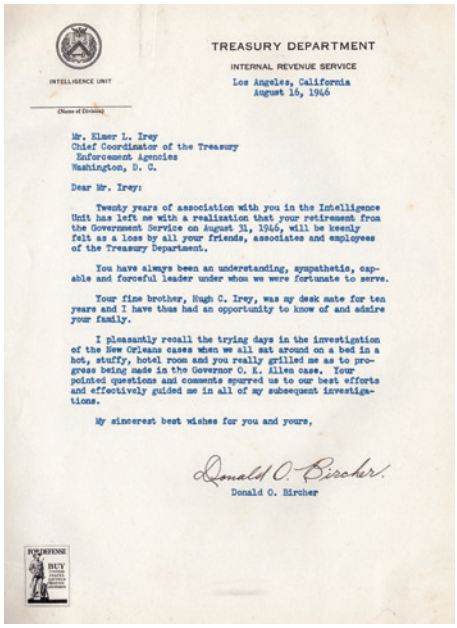
With best wishes and kind personal regards,

I am

Sincerely yours,

Dwight H. Green

GOVERNOR



TREASURY DEPARTMENT
INTERNAL REVENUE SERVICE
INTELLIGENCE UNIT
Los Angeles, California
August 16, 1946

Mr. Elmer L. Irey
Chief Coordinator of the Treasury
Enforcement Agencies
Washington, D. C.

Dear Mr. Irey:

Twenty years of association with you in the Intelligence Unit has left me with a realization that your retirement from the Government Service on August 31, 1946, will be keenly felt as a loss by all your friends, associates and employees of the Treasury Department.

You have always been an understanding, sympathetic, capable and forceful leader under whom we were fortunate to serve.

Your fine brother, Hugh C. Irey, was my desk mate for ten years and I have thus had an opportunity to know of and admire your family.

I pleasantly recall the trying days in the investigation of the New Orleans cases when we all sat around on a bed in a hot, stuffy, hotel room and you really grilled me as to progress being made in the Governor O. K. Allen case. Your pointed questions and comments spurred us to our best efforts and effectively guided me in all of my subsequent investigations.

My sincerest best wishes for you and yours,

Donald O. Bircher

Donald O. Bircher

However, Irey was not a pushover unwilling to give stern direction. Agent Donald Bircher wrote Irey, "I pleasantly recall the trying days in the investigation of the New Orleans cases when we all sat around on a bed in a hot, stuffy hotel room and you really grilled me as to progress being made in the Governor O.K. Allen case. Your pointed questions and comments spurred us to our best efforts and effectively guided me in all of my subsequent investigations."[13]

Leaders of character care for their people. In a group letter to Irey signed by six members of the secretarial pool, they told him, "Not one of us can recall a day when you weren't always willing to lend a helping hand; nor can we recall that you have ever been anything but our smiling Mr. Irey."[14] Former agent and U.S. Director of Procurement Clifford Mack perhaps best summed up Irey's compassion for his people. "I have always had a very pleasant recollection of the number of young folks who stopped by to visit with you and I noticed particularly that they invariably called you, 'Uncle Elmer.' I soon learned it was an expression of close friendship and desire to feel free to discuss their personal problems with you."[15]

Out of a sense of fairness, leaders of character ensure their people are credited justly for their hard work. James Olive—one of the Capone agents—told Irey, "Few men can look back upon achievements comparable to yours. Fewer still can do so with the satisfying realization that they gave full credit to all members of their organization who had a part in those achievements."[16] To Irey, this was just "simple justice."

Indeed, character alone will not give you complete competence. Like Hoover, Irey was a brilliant administrator with an attention to detail and noteworthy political savvy. But business acumen alone will not breed the fierce loyalty Irey generated. In his letter to the retiring Irey, Mike Malone—the ace undercover agent who gained the confidence of Capone and his henchmen—summed up the deep indebtedness many felt toward Irey: "Please do not hestitate to call upon me if I can be of service to you or your family at any time."

Irey's inspiration

Irey was not shy about who his inspiration was: the person who emancipated the slaves and successfully fought to hold the Union together, President Abraham Lincoln. According to Irey's granddaughter, Irey's home was filled with pictures of Lincoln. He even handed out pictures of Lincoln to his staff to inspire others.[17] When *Life* magazine came to photograph Irey for a featured article related to his retirement, Irey deliberately posed next to several pictures of President Lincoln that adorned his office.

President Lincoln said that, "No man is good enough to govern another man without the other's consent." Through his unwavering character, Irey earned the consent to lead others. Lincoln also said,

[13] Letter to Elmer Irey from Donald Bricher dated August 16, 1946, original in possession of Mob Museum.

[14] Letter to Elmer Irey from six members of Treasury secretarial staff dated August 1946, original in possession of Mob Museum.

[15] Letter to Elmer Irey from Director of Procurement Clifford E. Mack dated August 12, 1946, original in possession of Mob Museum.

[16] Letter to Elmer Irey from James Oliver dated August 14, 1946, original in possession of Mob Museum.

[17] Letter to Elmer Irey from Arcellus Shield dated August 16, 1946, original in possession of Mob Museum.

Elmer Irey ensuring files are in order and investigations are well documented.

"Nearly all men can stand adversity, but if you want to test a man's character, give him power." Irey was given the immense power to topple giants. However, he never abused it to build an empire, destroy his enemies or seek glorification. Instead, he judicially and fairly worked for a greater cause, which was the betterment of the nation. As the Governor of Illinois and former Capone prosecutor, Dwight Green, put it, "I feel that the people of our country owe you a great debt of gratitude."[18]

Irey did harness one power: the power of his character and with it he played a critical role in dissipating the culture of corruption and lawlessness that plagued the country during the 1920s. The Greek philosopher, Heraclitus, once said, "Character is destiny." Heraclitus believed—and history continually bears this out—that your destiny is not so much predetermined by fate but more so your character.

Officers of Intelligence Unit Bureau of Internal Revenue, Treasury Department, January 18, 1934.

If you choose to be a leader of character, you will define your leadership success. Your character is your destiny. However, character is not easily manifested overnight. It takes constant diligence to maintain your reputation of character. Doing the right thing sometimes is a lot more effort than the easy way out; but thanks to Irey we have a motivating tale of success. Who would have thought a climatic tale involving gangsters would have such a great leadership lesson?

Paul Camacho, CAMS, vice president of AML compliance, Station Casinos LLC, Las Vegas, NV, USA, paul.camacho@stationcasinos.com

[18] Letter to Elmer Irey from Governor Dwight Green dated September 2, 1946, original in possession of Mob Museum.

Regulating a game changer—Europe's approach to cryptocurrencies

Cryptocurrencies are seen as bringing innovation to the payments-services sector; furthering financial inclusion; and facilitating greater efficiency in cross-border transactions. However, as with other financial products and services, cryptocurrencies are also exposed to financial crime risks. The following article provides some background in relation to cryptocurrencies in general, and some insights into ongoing regulatory approaches and discussions in Europe.

Innovation and cryptocurrencies

According to a *Reuters* article published in February 2018, more than 1,500 cryptocurrencies are active around the world. In addition, hundreds of initial coin offerings (ICOs) who are seeking token buyers aim to join that list over the coming months and years.[1] By market capitalization, Bitcoin (at the time of writing) is the largest blockchain network, followed by Ethereum, Ripple, Bitcoin Cash and Cardano.

	CENTRALIZED	DECENTRALIZED
Convertible	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. *Example:* WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. *Example:* Bitcoin
Non-Convertible	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. *Example:* World of Warcraft Gold	Does not exist

Figure 1: According to the Financial Action Task Force (FATF), cryptocurrencies are a medium of exchange that operate in the digital space. They can be converted into either a fiat or it can be a substitute for real currency. Cryptocurrencies allow value to be transmitted globally without having to access a centralized banking system. There are two types of cryptocurrencies: centralized and decentralized which in turn can be distinguished into convertible and non-convertible.

Source: FATF Report: Virtual Currencies—Key Definitions and Potential AML/CTF Risks.

[1] "Cybercriminals target booming cryptocurrencies", *Reuters*, February, 1, 2018, https://www.reuters.com/article/us-cryptocurrency-cybercrime/cybercriminals-target-booming-cryptocurrencies-report-idUSKBN1FL5Q7

Beyond Bitcoin, the wider adoption of cryptocurrencies is still in its infancy but is likely to spread both into the traditional economy as well as throughout the sharing economy in the coming years. In order for mainstream adoption to take place, a regulatory framework, which protects all stakeholders, must also be developed. In the meantime, only minor regulatory steps have been taken, thus regulators regularly warn that investing in cryptocurrencies is high risk. In July 2014, the European Banking Authority (EBA) published an opinion on cryptocurrencies in which it outlines some 70 risks and makes recommendations on how to develop short and long-term regulatory measures to mitigate the risks.[2]

Governance and regulation

In May 2017, FATF held a Fintech and Regtech Forum that brought together 150 representatives from the fintech and regtech sectors, financial institutions, and FATF members and observers to address the regulatory and supervisory challenges posed by emerging technologies.[3] This initiative resulted in the guiding principles also known as the San Jose Principles.[4] In regards to cryptocurrencies, FATF encourages a risk-based approach. In its 2015 report, it provides an overview of the most widely introduced regulatory approaches, quoting the Bank for International Settlements' approach as follows:

- Imposing restrictions on regulated entities for dealing with cryptocurrencies
- Adopting legislative/regulatory measures, such as the need for exchange platforms dealing with cryptocurrency to be subject to regulation as money remitters, or the proposed regulation of cryptocurrency intermediaries in some jurisdictions for anti-money laundering/counter-terrorist financing (AML/CTF) purposes
- Publishing statements cautioning users about risks associated with cryptocurrency and/or clarifying the position of authorities with respect to cryptocurrency; and
- Monitoring and studying developments[5]

According to Global Policy Watch, the EU is assessing how blockchain and distributed ledgers technologies (DLT) can be used to improve transparency and manage the ever-increasing threats posed by cybersecurity risks amongst others. Given that the EU is supporting a number of projects in this area with the aim of harnessing the potential of this emerging technology, European institutions believe that it is too early to put in place a regulatory framework for blockchain technology.

A recent European Parliament Report on cryptocurrencies underlined that, "cryptocurrencies and DLT have the potential to contribute positively to citizens' welfare and economic development, including in the financial sector."[6] At the same time, however, the report also highlighted the risks noting that a regulatory framework will become important once DLT applications become systemically relevant. Of key importance is that the regulatory approach at the EU level is proportionate, so as not to stifle innovation or add superfluous costs at this early stage—while taking seriously the regulatory challenges that the widespread use of cryptocurrencies and DLT might pose. The report stressed the importance of any regulatory initiatives being equally as innovative as the technologies they aim to regulate, in order to be relevant and effective.[7]

The Fifth European AML Directive and cryptocurrencies

On July 5, 2016, the European Commission adopted a proposal to enhance the EU's anti-money laundering (AML) and counter-terrorist financing (CTF) framework. To prevent cryptocurrencies being used for the purpose of financial crime, the Commission aims to include virtual currency exchange platforms (VCEPs) and custodian wallet providers (CWPs) under the scope of the Fourth AML Directive (4AMLD),[8] whereas, virtual-to-virtual currency exchanges fall outside the scope of the amended 4AMLD.[9] VCEPs and CWPs will thus have to implement AML/CTF policies and procedures including adequate customer due diligence controls in order to be able to identify exchange's customers. The European

[2] "EBA Opinion on 'virtual currencies,'" European Banking Authority, July 4, 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

[3] "FATF FinTech and RegTech Forum 2017," Financial Action Task Force, May 26, 2017, http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-fintech-regtech-forum-may-2017.html

[4] Ibid.

[5] "Guidance for a Risk-Based Approach," Financial Action Task Force, June 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

[6] Jakob von Weizsäcker, "Report on Virtual Currencies," European Parliament, May 3, 2016, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0168+0+DOC+XML+V0//EN

[7] Jurgita Miseviciute, "Blockchain and Virtual Currency Regulation in the EU," Global Policy Watch, January 31, 2018, https://www.globalpolicywatch.com/2018/01/blockchain-and-virtual-currency-regulation-in-the-eu/

[8] "Commission strengthens transparency rules to tackle terrorism financing, tax avoidance and money laundering," European Commission, July 5, 2016, http://europa.eu/rapid/press-release_IP-16-2380_en.htm

[9] Jurgita Miseviciute, "Blockchain and Virtual Currency Regulation in the EU," Global Policy Watch, January 31, 2018, https://www.globalpolicywatch.com/2018/01/blockchain-and-virtual-currency-regulation-in-the-eu/

Commission's Vice President, Valdis Dombrovskis, was quoted as stating that the new rules mean "less anonymity and more traceability, through better customer identification, and strong due diligence."[10]

This was confirmed in April 2018 when the European Parliament adopted the Fifth AML Directive (5AMLD).[11] The 5AMLD extends AML and CTF rules to cryptocurrencies and will now apply to entities which provide services that are in charge of holding, storing and transferring cryptocurrencies. Therefore, cryptocurrency exchange platforms and CWPs are now required to implement know your customer procedures. Once the 5AMLD has been formally endorsed by the European Parliament and the Council, member states will then have up to 18 months to transpose the directive.

On February 26, 2018, the European Commission hosted a roundtable to debate the topic of cryptocurrencies.[12] The discussion touched on blockchain technology whilst noting that it holds strong promise for financial markets and that Europe must embrace this innovation in order to remain competitive. Concerns were voiced regarding the volatility and speculation around cryptocurrencies and ICOs' lack of transparency due to unknown factors regarding identity and underlying business plans as well as the risks which crypto-assets present with regard to money laundering and the financing of illicit activities. However, no concrete decisions were made as to whether and to what extent regulatory action at the EU level is required besides cryptocurrency exchanges and wallet providers being subject to the 5AMLD.

At an ACAMS Germany Chapter event hosted in Berlin on April 25, 2018, experts active in the cryptocurrency space joined a discussion on the risks and opportunities linked to cryptocurrencies as well as best practice approaches in regards to regulation. With experts joining from Poland and Germany, there was a general consensus to echo the current watch-and-see approach pursued by the regulators given that this is a burgeoning industry. Experts also raised the importance of establishing a unified taxonomy in order to develop a harmonized approach globally by more broadly enabling and facilitating the establishment of the cryptocurrency market. In terms of self-regulatory initiatives, varied organizations are active. In Germany, the Bundesblock[13] is a forum established some six months ago that also works on regulatory risk projects. On a more international scale, Global Digital Finance brings together cryptocurrency businesses, banks, regulators and industry experts in an attempt to develop a global approach. Some countries already appear to be putting in place a very attractive cryptocurrency regulatory framework and are thus preparing to attain a competitive advantage for when cryptocurrencies become better established. In this regard, it is worth quoting the Swiss Ministry of Finance, which recently stated that they want the ICO market to prosper without compromising standards or the integrity of the Swiss financial market.

> INTELLIGENCE AND LAW ENFORCEMENT AGENCIES CONTINUE TO SEE CRYPTOCURRENCIES BEING USED FOR THE PURPOSE OF FINANCIAL CRIME

Virtual crime investigations

Intelligence and law enforcement agencies continue to see cryptocurrencies being used for the purpose of financial crime. There is proof of established criminal and terrorist groups using cryptocurrencies on a large scale, though it seems they still rely on the more traditional and stable channels for money laundering such as cash or credit cards. However, the prospect that traditional criminal and terrorist networks could adopt cryptocurrencies more widely does pose a real concern. Albeit small in number, there have been cases which have demonstrated to law enforcement that money laundering and terrorist financing can take place within virtual realities where high levels of anonymity and low levels of detection are given, and thus removing many of the risks associated with real-world money laundering and terrorist-financing activities.[14] In early 2018, Europol announced that some 4 billion pounds ($5.4 billion) worth of cryptocurrencies have been laundered throughout Europe. Money laundering is one of several techniques that criminals use to obfuscate the movement of

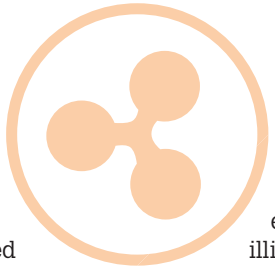
[10] "Remarks by Vice-President Dombrovskis at the Roundtable on Cryptocurrencies," European Commission, February 28, 2018, http://europa.eu/rapid/press-release_SPEECH-18-1242_en.htm

[11] "Statement By First Vice-President Timmermans, Vice-President Dombrovskis and Commissioner Jourovà on the adoption by the European Parliament of the 5th Anti-Money Laundering Directive," European Commission, April 19, 2018, http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm

[12] "Remarks by Vice-President Dombrovskis at the Roundtable on Cryptocurrencies," European Commission, February 28, 2018, http://europa.eu/rapid/press-release_SPEECH-18-1242_en.htm

[13] https://www.bundesblock.de/

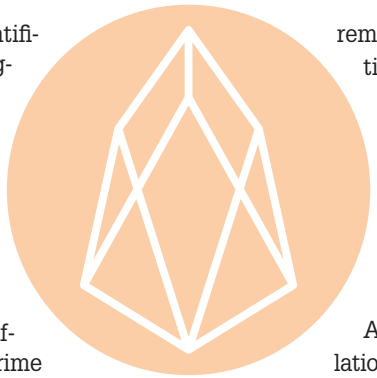
[14] David Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities" Royal United Services Institute, March 2017, https://rusi.org/sites/default/files/rusi_op_virtual_currencies_and_financial_crime.pdf



their assets so as to evade detection by authorities. Some have been known to utilize the Bitcoin blockchain for this purpose—attracted by its decentralized structure and notions of anonymity and pseudonymity.

A Royal United Services Institute report on cryptocurrencies published in March 2017 points out that governments understand that engaging with the cryptocurrency sector is key to help develop knowledge and insights into the legitimate uses of cryptocurrencies and the related technology. The cryptocurrency industry can also more effectively tackle financial crime if it understands the challenges and perspectives facing investigators and law enforcement agencies.[15] In September 2016, Europol, Interpol and the Basel Institute on Governance established a working group on money laundering and cryptocurrencies and to investigate and recover proceeds of virtual currency crimes.[16] The partnership has been developed as a network for information and knowledge exchange amongst European law enforcement agencies and other industry experts.

New challenges emerge for investigators and prosecutors when tracing, seizing and confiscating the proceeds of crime in cryptocurrencies.[17] On March 19, 2018, the Office of Foreign Assets Control announced that it might include specific cryptocurrency addresses associated with blocked persons as identifiers on the Specially Designated Nationals List, in order to strengthen its efforts to combat the illicit use of cryptocurrency transactions.[18] A number of companies (i.e., Coinfirm, Elliptic, Chainalysis, BitRank) specialized in the development of tools built specifically to investigate financial crime through cryptocurrencies have emerged in recent years. These firms are being used by companies and law enforcement to investigate financial crime activity and for AML purposes such as trying to establish the source of wealth of an individual whose wealth stems from cryptocurrency transactions.



Conclusion

Like the fintech sector overall, cryptocurrencies are laying the foundation for innovation in the payment space. Cryptocurrencies have legitimate uses and are thus attracting significant venture capital investment. The main attraction offered by cryptocurrencies is that they are seen as potentially being able to improve the efficiency of payments and thus reduce the costs for payments and fund transfers.[19] Like with traditional banking products and services, cryptocurrencies are exposed to the risk of financial crime.

Gary Gensler, one of the key regulators during Obama's tenure who is now at M.I.T., suggests that regulators are likely to scrutinize many of the current cryptocurrency projects. Although he claims that Bitcoin can remain exempt from securities regulations, he is of the opinion that Ether and Ripple, the second and third-most widely used cryptocurrencies, have most likely been issued and traded in violation of American securities regulations and will thus have to become compliant with U.S. securities legislation.[20] It is likely that European regulators will take a similar approach in terms of regulating cryptocurrencies and the activity linked to them.

With the arrival of cryptocurrencies along with other innovative approaches stemming from fintech, there is a consensus that putting in place strong public–private partnerships to improve AML/CTF is key in order to develop typologies and build a repository of red-flag indicators, and ultimately to pave the way for a sustainable cryptocurrency regime. A number of regtech companies are spearheading the development of cutting-edge investigative tools, which can support not only anti-financial crime investigations but also financial crime prevention in the cryptocurrency space.

Jennifer Hanley-Giersch, CAMS, managing partner, Berlin Risk Ltd., Berlin, Germany, jennifer.hanley@berlinrisk.com

[15] David Carlisle, "Virtual Currencies and Financial Crime: A Challenge and an Opportunity," Royal United Services Institute, December 6, 2016, https://rusi.org/publication/newsbrief/virtual-currencies-and-financial-crime-challenge-and-opportunity

[16] "Basel Institute, Europol and Interpol establish working group money laundering with digital currencies," Basel Institute on Governance, September 9, 2016, https://www.baselgovernance.org/news/icar/basel-institute-europol-and-interpol-establish-working-group-money-laundering-digital

[17] "The Aim of the Europol-Interpol Working Group" *Bitcoins Channel*, September 12, 2016, https://bitcoinschannel.com/europol-starts-group-to-study-cryptocurrency-launderers

[18] "OFAC FAQs: Sanctions Compliance," U.S. Department of the Treasury, April 13, 2018, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx

[19] "Guidance for a Risk-Based Approach," Financial Action Task Force, June 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

[20] "A Former Top Wall Street Regulator Turns to the Blockchain," *The New York Times*, April 22, 2018, https://www.nytimes.com/2018/04/22/technology/gensler-mit-blockchain.html

Hard times for whistleblowers

In 2015, ACAMS' European account manager David Sanchez Lopez, based in France, met Stéphanie Gibaud at an ACAMS networking event in London, U.K. The ACAMS France Chapter is always keen to invite personalities who play a major role in any area linked to compliance matters and was therefore very excited at the mere thought of talking to Gibaud about her experience as a whistleblower.

In the collective mind, the one who "blows the whistle" is a kind of Robin Hood who dares to attack the system. He or she is very ethical, has strong moral values and wants the community to be informed of all sorts of wrongdoings and malfunctions taking place behind the curtain and behind its back.

However, reality is far from glamourous. When meeting Gibaud, the chapter realized a whistleblower is a person who effectively proclaims secrets from the rooftops but at the same time, jeopardizes their whole life.

Every case is its own and the mere nature of the alert, the sector concerned or the locale seem to play a prominent role. The secret data of the leak can turn out to be financial information; everybody remembers the Panama Papers and the Paradise Papers. It might relate to scandals in the medical field or to corruption at the state level. It can relate to bad treatment within the army or to financial misuse of resources allocated to an embassy. The disclosure of activities where information on illegal activities is being kept secret will do.

Whistleblowers can be anyone. They can be you and me. They can be found at any level of the social scale. They have something in common though: an above average consciousness of their citizenship that nearly always gets them into private and public troubles.

What happened to Stéphanie Gibaud?

In March 2018, the chapter had some difficulties locating Gibaud as she had changed her known location. After weeks of unfruitful attempts to contact her, the chapter was about to give up on having her speak at a conference when she unexpectedly called back.

The chapter met Gibaud, their French Erin Brockovich,[1] at 8 a.m. The good-looking mother of two was very elegant and full of energy. She joined the chapter for breakfast at a hotel near the Eiffel Tower and explained that she knows Paris very well

[1] Erin Brockovich is known for her involvement in one of the largest direct action lawsuits in U.S. history, http://www.brockovich.com

because she used to work and live in the city, just around the corner from the event. "I had a comfortable life before all that happened, 10 years ago," she said.

She previously had professional status, financial security and traveled around the world to represent the bank where she was formerly employed. The chapter was astounded by her professionalism.

She explained, "As a public relations specialist, if I had shredded the documents UBS (France) SA suddenly asked me to destroy in 2008, I could have risked prison. I was working for the UBS marketing department and had absolutely no idea of the scope of the documents I was supposed to get rid of. Searches were taking place; I refused to be part of illegal activities and blew the whistle internally. Weakened by the harassment I was suffering at UBS, I was targeted by the French state in 2011 and, constrained by the law I was obliged to communicate confidential information to the Ministry of Finance, which has widely helped to identify numerous offshore bank accounts."

The Swiss wealth management bank "UBS AG" created UBS SA in France back in 1999. The Swiss market was limited and the bank wished to develop its activities abroad. However, in the summer of 2007, the head of internal audit of UBS (France) SA shared his suspicions with several local executive management team members.[2] He suspected that various Swiss portfolio managers convinced French wealthy clients living in the nation into investing in Switzerland, where—at the time—banking secrecy was still very strong and, in doing so, promoted tax evasion. Internal audit could not reconcile the gap detected between funds officially collected and the amounts taken as a basis to calculate the bonuses of some of these portfolio managers. This gap aroused suspicions.

Shortly after, an anonymous letter concerning UBS (France) SA landed on the desk of the French supervisor.[3] The agency started an investigation. A sanction of €10 million euros and official charges were filed against the French subsidiary of the Swiss bank as a result of the investigation.

Gibaud refused to follow the orders of her management to destroy data and ended up lodging a complaint against her employer. In doing so, she became part of the whistleblowing process.

A schizophrenic system

The information Gibaud exposed largely helped the French Ministry of Finance identify 38,000 offshore accounts, held by French citizens, worth €12 billion euros. This is what Gibaud said and this is what the chapter heard the French finance minister say on TV during her presentation. The minister looked her in the eye as he thanked her for her worthy contribution.[4]

One would think the French state would be grateful for such an unexpected "coup" and would help Gibaud find a new position after she was laid off by her former employer.

Nothing was further from the truth. Today, Gibaud is in a precarious situation. Her every attempt to dive into the employment market again has failed. Financial institutions and other employers probably fear she will blow the whistle on them.

On the one hand, Gibaud has received numerous accolades. It seems society does recognize the value of her contribution to the community at large and has granted her various opportunities to highlight her heroic actions. "After publishing my first book in 2014, *La femme qui en savait vraiment trop*,[5] I received the Anticor prize and was nominated for the Sakharov prize with Snowden[6] and Deltour[7] in 2015," she recalled. On a political and judicial level, she receives great attention from the French authorities. In 2015, she was invited to speak in parliament in Brussels within the frame of the "Tax Rulings" commission.

Nonetheless, Gibaud remains totally isolated. She fights to make a living. On her situation, she said, "I am not employed at any job. In other words, in our society, I am a no-one." However, she very quickly adds, "I won't give up. I will keep fighting. I have just created my own structure."[8]

Would Stéphanie be better off if she were an American citizen?

"Disclosing wrongdoing can be a daunting undertaking that can lead to a loss of livelihood and professional marginalization. In addition to the stigma that may be attached to blowing the whistle, employees may also

[2] "Autorité de Contrôle Prudentiel et de Résolution, procédure 2012-03," UBS (France) SA, June 25, 2013, https://acpr.banque-france.fr/sites/default/files/medias/20130626-decision-de-la-commission-des-sanctions.pdf

[3] Autorité de Contrôle Prudentiel et de Résolution, https://acpr.banque-france.fr/

[4] *Cash Investigation*, «Panama Papers – Paradis fiscaux: le casse du siècle,» April 5, 2016, https://www.francetvinfo.fr/replay-magazine/france-2/cash-investigation/cash-investigation-du-mardi-5-avril-2016_1381113.html.

[5] Stéphanie Gibaud, *La femme qui en savait vraiment trop*, 2014.

[6] Edward Snowden copied and leaked classified information from the National Security Agency (NSA) in 2013 without authorization.

[7] Antoine Deltour is behind the disclosure of many of the LuxLeaks documents, https://support-antoine.org/en/#luxleaks

[8] Stéphanie Gibaud is president of ETICARE, www.stephaniegibaud.org

fear financial and reputational degradation. In order to curtail these potential losses and encourage individuals to come forward in the detection of wrongdoing, countries have introduced various incentives, ranging from tokens of recognition to financial rewards," said the Organization for Economic Co-operation and Development (OECD).[9]

Bradley Birkenfeld can give evidence of the "financial rewards" mentioned in this OECD report. Birkenfeld was the UBS wealth manager who blew the whistle on illegal offshore accounts held in Switzerland by U.S. citizens, and as such, closely resembles the U.S. counterpart of Gibaud. Birkenfeld's disclosures to the U.S. government triggered an investigation against UBS, which was suspected to have enabled tax evasion by U.S. taxpayers. In February 2009, based on the information given by Birkenfeld, the U.S. Department of Justice announced, "The successful negotiation of an agreement that…result[ed] in the IRS receiving an unprecedented amount of information on United States holders of accounts at the Swiss bank UBS."[10] A deferred prosecution agreement was reached with UBS. A total of $780 million in civil fines and penalties was paid by UBS. The release of previously privileged information on American tax evaders was included in the package.

Just a "tiny" difference between Birkenfeld and Gibaud: as a result of the financial repatriation facilitated by his whistleblowing, Birkenfeld received a $104 million award from the IRS Whistleblower Office in September 2012.[11]

Gibaud would definitely be better off if she were an American.

A law to protect whistleblowers

Two different stories, two different places, two different endings. As is often the case, the story of a corruption scandal is initially heard via the media and people tend to only pay attention to the headlines until they meet someone who is involved in its unfolding. That is when people start becoming aware of the fine print of their legal system and how those rules might one day affect them.

To adequately assess the treatment of whistleblowers in your specific country, consider the following criteria: financial rewards, protection of whistleblowers, anonymity, internal vs. external reporting processes, etc. French legislation seems to cover each of these aspects, except financial rewards.

Whistleblower protection was integrated in France in the Sapin 2 law.[12] The law says that to blow a whistle you need to adhere to the following procedure: you must inform your manager and if they do not react, inform the authorities. If nothing happens within a month, you can go public with your whistleblowing or you can contact the defender of rights.[13] The anonymity of the whistleblower is ensured. The job application of a former whistleblower is not allowed to be dismissed. A whistleblower can be reintegrated in their former position. Last but not least, private and public companies corresponding to certain characteristics (a specific size and the location of their headquarters) have the obligation to implement a system that makes it possible for individuals to raise suspicions. The law came into force in December 2016.

Unfortunately, any whistleblowing before December 2016 is out of the scope.

Thank you very much for your sacrifice, Ms. Gibaud

The price to pay for whistleblowing is very high. Gibaud lost her employment at UBS, and consequently her assistant and salary. She now gives interviews, participates on TV shows and meets with other whistleblowers. For the last 10 years, she has continued raising her voice in part by commenting on the emblematic cases of Edward Snowden, Chelsea Manning and Julian Assange in her last book.[14]

On a separate note and overall, Birkenfeld's case was a good deal in the long-run for the whistleblowing community. Have not the lines moved? The Birkenfeld case is considered to be the starting point of the erosion of Switzerland's banking secrecy. In addition, Switzerland signed the Convention on Mutual Administrative Assistance in Tax Matters on October 15, 2013.[15]

The chapter wonders whether Gibaud will ever work in the financial field again, or find a steady job. The word "sacrifice" is the only word that comes into everyone's minds when thinking of Stéphanie Gibaud.

Nathalie Bosse, CAMS, communications director, ACAMS France Chapter, Paris, France, nbosse@acams.org

[9] "Committing to effective whistleblower protection highlights," Organisation for Economic Co-operation and Development, http://www.oecd.org/corruption/anti-bribery/Committing-to-Effective-Whistleblower-Protection-Highlights.pdf

[10] "IR-2009-75," Internal Revenue Service, August 19, 2009, https://www.irs.gov/newsroom/irs-to-receive-unprecedented-amount-of-information-in-ubs-agreement

[11] Andrew Krieg, "October 2016 News Reports," Justice Integrity Project, https://www.justice-integrity.org/news-reports?start=18

[12] "Loi 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique," Legifrance, December 10, 2016, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033558528&categorieLien=id

[13] http://defenseurdesdroits.fr

[14] Stéphanie Gibaud, *La traque des lanceurs d'alerte*, Max Milo éditions, 2017. The book is prefaced by Julian Assange.

[15] "Switzerland Deposits Instrument of Ratification of OECD Multilateral Convention on Mutual Administrative Assistance in Tax Matters," World.Tax, March 10, 2016, https://www.world.tax/news/switzerland-deposits-instrument-of-ratification-of-oecd-multilateral-convention-on-mutual-administrative-assistance-in-tax-matters.php

Be confident in your next business move with CLEAR®.

Thomson Reuters CLEAR® investigative due diligence solution helps you quickly and easily filter untrustworthy data, meet increased demand, and avoid incomplete research. Identify hard-to-find risks and create connections to optimize your AML/KYC program.

With CLEAR, you get the confidence that only comes from trusted answers.

Learn more at legalsolutions.com/AMLsolutions

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®

The data provided to you by CLEAR may not be used as a factor in establishing a consumer's eligibility for credit, insurance, employment purposes or for any other purpose authorized under the FCRA.

EUROPEAN CONNECT: JUNE–AUGUST 2018

During July and August, many of you will be taking two or three weeks away from the office to relax, recharge and reconnect with friends and family. I will certainly be doing that this year and I am keeping my fingers crossed for a sunny few months.

For those quieter moments back in the office, why not take the time to recharge your professional knowledge? Our certificate courses are taught live online, and are a great way to earn Certified Anti-Money Laundering Specialist (CAMS) credits toward CAMS certification or recertification—all without leaving the office.

In 2018, we launched three-brand new certificates tailored for European compliance professionals of virtually any level of seniority.

- AML for Fintechs
- Fintechs as Your Customers
- GDPR and 4AMLD

AML for Fintechs

- This course was created specifically for compliance professionals currently working in EU fintech organizations, to help them understand how to meet their important anti-money laundering (AML) obligations
- It is also relevant if you aspire to work for a fintech, as it will give you a great base for understanding how this innovative sector is unique in the world of anti-financial crime

Fintechs as Your Customers

- Unlike AML for Fintechs (which is designed for those working in fintechs to understand AML principles and best practices), this course is designed for compliance professionals in conventional organizations who have fintechs as their customers
- It answers questions like "What is a fintech?" and "How is their governance different from other sectors?" but also gets very practical around issues like know your customer, data storage and more
- This is the ideal certificate for entire anti-financial crime teams to take, to make sure you are on the same page as your EU digital business customers

GDPR and 4AMLD

- The EU's solution to modernize data protection takes the form of the new EU General Data Protection Regulation (GDPR), which came into effect on May 25, 2018. The GDPR essentially unifies the 28-member states approach to data protection laws
- This certificate course aims to provide practical guidance on how to comply with both AML and GDPR requirements, and it is suitable for everyone from the board, to legal, to compliance

If any of these sound right for you, you can find out more and register at www.acams.org/certificates. In addition, if you are a team leader who would like to train your entire team on one of the specialized topics in which we offer certificates, call our London office at +44 20 3755 7400 to discuss group pricing. Use summer 2018 to recharge your professional expertise!

Angela Salter, Head of Europe, ACAMS, London, U.K., asalter@acams.org

Fintech Avenue

SAR NARRATIVES: LAW ENFORCEMENT EXPECTATIONS

The Northern New Jersey (NJ) Chapter hosted an event on March 29, 2018, titled SAR Narratives: Law Enforcement Expectations. The NJ Chapter coordinated this event to get a better understanding of what law enforcement would like to see in suspicious activity reports (SARs) to ensure financial institutions are providing valuable financial intelligence. The ongoing dialogue between law enforcement and financial institutions helps improve investigations and SAR decision-making, and educates the AML community on what information is important to include in the SAR narrative.

What better way to learn what is needed on SARs than to hear it from the party that actually uses the SARs for their investigations? The NJ Chapter had IRS Special Agent Michael McGarry present on the topic. Agent McGarry is currently the lead agent for the IRS' Financial Crimes Task Force with 15 years of experience in money laundering and tax evasion investigations and holds a wealth of knowledge in Bank Secrecy Act (BSA) violations. In addition, Agent McGarry is the Newark Field Office BSA coordinator, overseeing the U.S. Attorney's SAR review team of New Jersey.

During the event, we learned that there are SAR review teams throughout the country that consist of different law enforcement agencies, such as the FBI, IRS, Drug Enforcement Agency (DEA) and Department of Homeland Security (DHS). All SARs that are filed to the Financial Crimes Enforcement Network are reviewed by these teams based on the jurisdiction of where the SAR was filed. After reviewing the SARs, the agencies decide which cases they want to pursue for further investigation. Some cases are pursued by one agency. However, if multiple civil and/or criminal violations are found, then some cases are investigated jointly. For instance, if a SAR implies that tax evasion is the suspected suspicious activity, then this case will be pursued by the IRS. If a SAR is filed on illicit funds possibly derived from human trafficking and drug trafficking, then this case will be pursued by both the DHS and the DEA. Once it is decided that further investigation is needed, the supporting documentation is requested from the filing institution.

Another highlight of the event was learning what information to include in the narrative section of the SAR. In addition to giving a detailed description of the transactions that took place in an account, the institution should also use the narrative section to describe why the activity is suspicious. This will grab law enforcement's attention as they read the SAR. The more information provided on the suspicious activity, the better. The chapter also learned that it is preferred to submit an attachment of the transactions with the SAR rather than putting a lengthy list of transactions in the narrative section. If many transactions are involved, then a paragraph summary is preferred over a bullet-point list of transactions along with a comment in the narrative stating that there is an attachment to the SAR.

The chapter also learned that if an institution is closing an account, the narrative should include the closing balance of the account and if possible, where the funds went. In an instance where the SAR case is being pursued, law enforcement would also like to know where the funds went in order to follow the money trail. In addition, if an institution feels that a particular SAR case needs immediate attention and if their bank policy does not restrict this, then the institution should contact their local police department. Agent McGarry also shared interesting money laundering cases that derived from SARs that were filed as well as tips and red flags to look for when an institution is conducting an investigation.

Overall, the event was very informative and educational. The attendees of the event consisted of other law enforcement agents, compliance officers from banks, money services businesses and consultants. The attendees asked several questions related to their respective industries. Many chapter members also shared past experiences with money laundering cases they have dealt with and SARs they have filed. As a result, this was a great learning experience for everyone.

The NJ Chapter has partnered with law enforcement to educate the AML community. We recently had an event on human trafficking presented by Keith Kolavich, group supervisor of the human trafficking unit of DHS. This was also a successful event with positive feedback from many NJ Chapter members. The NJ Chapter has lined up exciting upcoming events for this year with the New Jersey Financial Crimes Bureau of the Department of Criminal Justice and High Intensity Financial Crime Area/High Intensity Drug Trafficking Area agents. Please visit our chapter webpage on acams.org for chapter updates.

Desiree Santiago, CAMS-FCI, AVP AML officer, Metropolitan Commercial Bank, New York, NY, USA, dsantiago@mcbankny.com

SARs Place

DENISE NOVA:
Event planning and technology

ACAMS Today chatted with Denise Nova, ACAMS' event logistics supervisor, about planning ACAMS conferences and her favorite event.

Nova was born and raised in Miami, Florida. She initially studied human resources administration, but decided to take a different career route. She worked in different industries until she found her niche in event planning. Nova worked for seven years at The Ritz-Carlton Key Biscayne catering department. She held several positions and eventually became the lead event concierge. Later, she worked as the catering manager at the Crowne Plaza Hollywood Beach for three years. After 10 years in event hospitality, her career led her to corporate planning. Nova has worked at ACAMS for six years as the event logistics supervisor.

ACAMS Today: As event logistics supervisor, what does your job entail on a day-to-day basis?

Denise Nova: As an event logistics supervisor, I am responsible for managing the program logistics for all ACAMS events. I oversee a team of event coordinators to ensure the successful execution of speaker, sponsor, exhibitor and third-party vendor logistics for ACAMS annual conferences.

In addition, my role requires daily collaboration with key stakeholders, which is essential to ensure project deadlines are met and to ensure the success of each event.

AT: ***How have ACAMS conferences evolved since you first began your position?***

DN: ACAMS has established themselves as a leader in providing robust content, which has not changed. However, in the last six years, we have definitely seen a change in the way we deliver this information. ACAMS conferences have become more innovative, with added technology. Through livestreaming, we have been able to accommodate people who are not be able to travel to the conferences. We have also added the mobile app, which means that attendees can have access to the latest information at all times, with real-time updates.

The mobile app project was also an opportunity for me to evolve personally, as it forced me to update my cell phone and learn about not only using, but also building an app.

AT: ***What is your team's organizational secret to making sure all the conferences run smoothly?***

DN: I owe the success of my team to our communication and organizational skills. We make it a point to be informed and prepared for tasks and responsibilities we must tackle as a team. It is the passion we have for our conferences to be successful that drives the entire operation.

AT: ***What is your favorite conference and why do you like attending this specific conference?***

DN: The Latin-American conference in Cancun is my favorite for obvious and nostalgic reasons. Obviously, who wouldn't enjoy a conference in Cancun? The setting is magnificent and the culture of the attendees is so warm and friendly that you almost forget that you are working. It is also one of the first conferences that I coordinated from beginning to end and was onsite for, when I started at ACAMS six years ago. Being able to go back there every year reminds me of that sense of pride and accomplishment I had the first time I successfully planned and executed that event.

AT: ***When you are not planning conferences, what do you like to do in your spare time?***

DN: My dream is planning events. So, when I am not planning successful and informative conferences, I am planning life celebrations for my friends and family. I come from a large family, so there is always an event on the horizon.

Also, because I worked in the food and beverage industry for so many years, I developed a love for wine and plan annual vacations to do just that—wine tastings. I love to taste and collect new wines.

Interviewed by: Karla Monterrosa-Yancey, CAMS, editor-in-chief, ACAMS, Miami, FL, USA, editor@acams.org

Stephanie Trejos, editorial assistant, ACAMS, Miami, FL, strejos@acams.org

ACAMS® | Conferences

Viva the Future!
Acing the New AML

AML is an ever-changing profession with rapidly evolving regulations, technology and financial crime methods such as cyberattacks.

ACAMS 17th Annual
AML & Financial Crime Conference

October 3 – 5 | Aria Resort & Casino | Las Vegas, Nevada

Register Today:

www.acamsconferences.org/vegas

info@acams.org

ADVANCED CERTIFICATION GRADUATES

Australia
Crispin Yuen, CAMS-Audit

China
Jianguo Hu, CAMS-FCI
Na Li, CAMS-Audit
Sichen Liu, CAMS-Audit
Xin Wang, CAMS-Audit
Zhengyan Wu, CAMS-FCI
Teng Zhang, CAMS-FCI

Curacao
Natasha Blomont, CAMS-FCI
Marisol De F. Pereira, CAMS-Audit
Genesis Martis, CAMS-FCI

Guyana
Wayne Razah, CAMS-FCI

Hong Kong
Ting Fung Ting, CAMS-FCI

India
Farokh Adarian, CAMS-FCI
Ramesh T. Ramanan, CAMS-Audit

Japan
Aya Kishie, CAMS-FCI
Yu Komuro, CAMS-Audit
Sanae Tokita, CAMS-Audit
Toru Yamazaki, CAMS-Audit

Liberia
Gabriel W. Bellepea, CAMS-Audit

Malaysia
Boon Kin Lau, CAMS-FCI

New Zealand
Tijana Misur, CAMS-Audit

Nigeria
Barineka Thompson, CAMS-Audit

Singapore
Cynthia Cheong, CAMS-Audit
Pooja Dash, CAMS-Audit
Christophe Lacroix, CAMS-Audit
Fay Robinson, CAMS-Audit
Charlene Su, CAMS-Audit

Taiwan
Chia Chi Cheng, CAMS-Audit
Hsiao-Chun Han, CAMS-Audit
Yi-Chang Liu, CAMS-Audit

Thailand
Somsiri Siyarngnork, CAMS-Audit

United Arab Emirates
Altaf Shaikh, CAMS-FCI

United Kingdom
John Oridupa, CAMS-Audit

United States
Emil Ivanov, CAMS-Audit
Scott Karem, CAMS-FCI
Benay Nachin, CAMS-FCI
Richard Ricot, CAMS-Audit
Christopher Rowland, CAMS-FCI
David Ryan, CAMS-FCI
Desiree Santiago, CAMS-FCI
Marina Slavova, CAMS-Audit
Jamie Thomas, CAMS-FCI
Monika Wilejto-Rieken, CAMS-FCI
Nella Zelensky, CAMS-Audit

CAMS **GRADUATES**: FEBRUARY–APRIL

Albania
Alketa Mustaka

Andorra
Francesc Josep Girau Rodriguez
Ferran Tunez Parisi

Argentina
Paula Barnes
María Agustina Capellades
Gabriel Martin Rodriguez

Armenia
Maria Galstyan
Sos Hakobyan

Aruba
Marilyn Emily Grant

Australia
Richard Baker
Tiffany Chien-Ling Chiu
Juan Correal
Patrick Gallagher
Susana Irene Garcia
Naren Kartikey
Taha Khan
Nicole Pak Yiu Leung
Chizu Lockey
Emma E. Murphy
Cameron R. Paterson
Shen Yu-Hsuan
Lakshmi Suthakar
Jana Svecova
Anita Chai Hoon Ting
Belinda M. Worrell

Bahamas
Tanya Cecile McCartney

Bahrain
Eyad Nadhem Al Saleh
Fatima Al Shoala
Amal Jamal Hameed Almarhoon
Ahmed Abdulla Ayyad
Muhammad Imran
Javed Iqbal
Anjani Kumar
Nisha Nair

Bangladesh
Md Abdullah
S M Tarik Ul Alam Pavel
Pritish Barua
Kazi Mahbub Hasan
Ahmed Saiful Islam
Ashiqul Islam
Rashadul Karim
Mohammad A. Shaon

Barbados
Jamila Aisha Bradshaw
Judith Sarjeant

Belgium
Stefano Siggia
Barbora Zvadova

Benin
Catherine Amarachi Martins
Enongande N. Edith Somasse

Bermuda
Kemda R. Bean
Nakia Koshea Scott-Millett

Bolivia
Leidy Diana Carrasco Ordonez

Botswana
Kagiso Mochabaki

Brazil
Alberlei I Aparecido De Oliveira
Maria A. De Marco Bohomoletz
Peterson Cis
Raphael Dogani
Keron Cecchini Marques
Fabio Sarabia

Bulgaria
Iliana Byanova
Iskra Edreva

Cabo Verde
António S. W. V. Soares Monteiro

Canada
Olurotimi Akinsanmi
Ayisha Ali
Tara-Lee Andrew
Sylvie Archambault
Donna Bales
Octavian Barbu
Anne-Gaëlle Baroni
Stanislav Belilovskiy
Himanshu Vyomesh Bhatt
Ana Boras
Aida Bou-Daher
Nicole D. Briscoe
Donna Brown
Donna Bullard-Pease
Dolly Carolina Cedeno
Peter Chan
Philip Cheung
David Colantonio
Ciara Marie D'Arcy
Rominder Singh Dhonsi
Cesar A. Felix Suriel
Leanne Fernandes
Ronnie Fernandes
Maude Frenette
Todd Gilham
Jonathan Karanja Gitiya
Rudresh G. L. Gowda
Srirajah Gunarajah
Carol A. Hall
Simon Zee-Tat Huang
Michael Hull
Ismahan Ibrahim
Phillip Jarrett
Jairaj Singh Jolly
Veronika Kapel
Ali Kiani-Felavarjani
Sakana Kiritharan
Yongsuk Andrew Kwon
Erin Kirsten Lam
Yau Wing Lam
Yuan Lan
Ryan V. LaRose
Tingting Lu
Marina D. Madzarevic-May
Michel Mesia
Brian Moreau
Rekha S. Nair
Saritha S. Nair
Mai N. Nguyen
Bernard Norris
Olutobi Adeleye Oyedeji
Rajinder Rai
Abbas Rajabali
Michael Ramsay
Karthigesu Ravendran
Blair A. Riedlinger
Kimberly M. Rome
Neil Sadiku
Sohel Saleh
Lorena Saracino
Michelle J. Sarmiento
Manjinder Shoan
Melissa Shum
Priscilla Silva Borges
Omesh Singh
Mélissa Sivret
Ehab Taha Mahmoud
Joyce L. Teoh
So Yin Anna Tsui
Badri Babu Varadarajan
David Vijan
MeiMei Wang
Zeeshan Waraich
Chung Yan Wong
Heling Yang
Christopher Yasin
Celine Hoi-Yan Yeung
Menaha Yogathasan
Syed Shahzad Haider Zaidi
Lena M. Zecchino
Maryssa Zelden

Cayman Islands
Nikita Kissoon
Benjamin Tynan Marler
Nathania Pearson
Andy Spilsbury
Breda Mary Verling

Chile
Nicolás S. Recabarren Alarcón

China
Ying Tung Chan
Shu-Hsia Chang
Hao Chen
Wei Chen
Yi Fan
Li Yun Gao
Bingqian Ge
Jianmei Guo
Bin He
Jing He
Xiaoyun He
Chen-Yuan Hsu
Zi-Cheng Hsu
Yandi Huang
Yu Xian Huang
Wei Li Jing
Juihsia Kao
Huey-Fen Lay
Che Hung Lee
Jiajia Li
Lan Li
Ruhan Li
Shukui Li
Tingting Li
Yudong Li
Jiemin Lin
Hsun-Chieh Liu
Zhiping Liu
Shih-Sung Lo
Meng Lu
Shiying Lu

Deyi Luo
Li Luo
Chia Jung Ma
Yun Mao
Junxiang Niu
Hui-Ting Pao
Haimiao Qu
Bizhou Shi
Chao Shi
Shuang Su
Jingyi Sun
Kang-Lin Tsai
Shi-Fong Tsai
Jin Wang
Tingting Wang
Bingru Wu
Jian Min Wu
Xue Xia
Jingyao Xiao
Wen Xiao
Ruijie Xu
Heng-Chuan Yang
Jieqing Yang
Shixuan Yu
Yuan-Chi Yu
Hong Zhang
Jiahui Zhang
Kai Zhang
Xinyun Zhang
Yun Zhang
Bozhong Zhao
Jie Zhao
Wenting Zhao
Yan Zheng
Yuanyuan Zhu
Weiwei Zuo

Colombia

Yerson Lopez
Sandra Milena Meza Cuervo

Congo

Jeff Mukadi

Curacao

Luranne Kayly Falconi
Juweel A.M. Soleana

Cyprus

Athena Yiallourou

Czech Republic

Pavel Dlouhy

Denmark

Brian Wihrenfeldt Andersen

Dominica

Annette L. Lestrade

Dominican Republic

Rosmery Alba

Egypt

Kareem Ragaey El Ganainy
Inas Abdel M. El-Ghamrawy
Kholoud M. Hussein

Estonia

Chantele Ford
Jorgen Kaarnamets
Dmitry Kuravkin

Finland

Heikki Koivupalo
Jenna Makinen
Matti Tormanen

France

Edem Adjete
Anne Sophie Bouyssou
Raphael Cavrois
Tugdual Chevalier
Amandine Ciurletti
Laurent De Monneron
Hélène Dieul
Luc Douezi
Louis-Jean El Gammal
Christophe Gilles
Eliane Kambire
Beatrice Kraszewski
Patricia Lagadec
Helene Luciani
Frédéric Mouzat
Nathalie Nagre
Magueneï Pari
Aurélie Ranouil
Imran Raza
Celia Savigny
Valentin Thomas
Hiroshi Yamashita

Georgia

Nato Moroz

Germany

Silvia-Andreea Awad
Christian Bader
András Borsföldi
Axel Detering
Ting Li
Luisa Malcherek
Altamash Rahman
Amr A. Kamel Moussa Salman
Sven Scholz
Niina Toikkanen
Thomas Witter
Maria Zeizinger

Ghana

Godfred Abakah
Deborah Naa Deide Aryee
Meshach Hagan

Greece

Torsteen Overgaard

Guyana

Niranjanie Ramprashad
Alicia O. Williams

Hong Kong

Yan Chui Au
Emma Bousfield
Xiaoqian Cao
Aretha Chan
Cheung Hung Chan
Ka Pou Chan
Ka Yan Karen Chan
Kwan Ming Chan
Man Ning Luna Chan
Wai Kuen Chan
Yiu Lai Chan
Yuen Ki Chan
Yuk Chi Chan
Pik Wai Beverly Chen
Ho Cheng
Wing Lam Cheung
Ya-Chi Chiu
Song Wan Choy
Kit Ling Chung
Yu Ting Fung
Shih-Ping Gue
Anthony Lok Yee Ho
Yiqing Hong
Chui Ying Hung
Tsz Sum Ip
Mark Kim
Man Ming Kot
Cheuk Yu Kwan
Siu Ping Kwan
Fu Kit Kwok
Chi Chung Lai
Man Dik Lai
Chun Him Lam
Wing Yan Lam
Chung Yan Lan
Ka Wing Lau
Kit Ming Law
Tak Chuen Lee
Calvin Hon Tao Lei
Kai Chung Leung
Shiu Wing Leung
Chun Man Li
Shu Hua Lin
Cho Yan Joanna Liu
Hin Yau Eric Liu
Hau Yee Liu
Tze Ying Liu
Chun Yin Luen
Chi Ning Lui
Samuel Wai Lap Lung
Le Lu
Malgorzata Maciuba Phalaris
Matthew Mcaleney
Leo Wang Yip Mui
Ka Chun Clarence Ng
Kwok Ho Ng
Pik Sai Ng
Yanty Ng Yau Ling
Juan Angel Otero Somoza
Chi-lun Pang
Tsun Kit Pang
Tyler J. Pederson
Olivia Won Wai Poon
Nihal Manikant Shah
Jiayi Shen
Wai-Ling Suter
Wai Lok Ivan Tam
Max Ka Wai Ting
Yi-Ching Tsai
Kwok Wai Tsang
Wai Han Tse
Kenny Kawai Tsim
Wing Yin Tsoi
Shing Wan Tsui
Lonneke van Zundert
Wai Sze Wan
Ching I Wang
Lingfei Wang
Shu Yuan Wang
Hsiu-Chuan Wei
Chun Fat Wong
Hoi Yi Helen Wong
Ka Mei Wong
Hiu Shuet Wong
Wai Shuen Wong
Chiu-Hui Wu
Xiaofan Wu
Yunjing Xie
Louise Wing Lam Yam
Tsz Lok Yeung
Ka Yan Yip
Yuk Ching Yip
Elaine Yu
Tsz Shan Yu
Karen Ka Yan Yuen
Pui Hin Brian Yun

Hungary

Jimuzi Zhou

India

Soloman Raj Akana
Shibu Arumugam
Siddhartha Prakash Biyani
Annesha Bose
Manu Chandna
Shivakumar Chandran
Ashwani Changra
Tejas Chotalia
Chandan Das
Sumit Dhar
Deanne Drego
Lancy D'Souza
Michelle D'souza
Vijay M. Gaba
Manish Kumar Gautam
Rahul Gop
MohanRaj G
Prabhat Gupta
Prachir Gupta
Meera Rajesh Iyer
Hari Ganesh Jagan
Shiva Kiran Jakkula
Pankaj Kandwal
Deepti Kapoor
Amit Karwasra
Shobhit Khaitan
Mukund Arvind Kurundkar
Chandrashekhar Kushwaha
Khuzema Lehri
Bharanidharan M
Kusha M N
Ravi Shankar Mallavarapu
Namrata Manjhi
Prakash Chandra Mishra
Priyanka Mohanty
Yuvaraj Moorthy
Sarita Nair
Shobha Nair
Neetu Sushil Nembhani
Suresh Anand Neralla
Pramod Kumar Nimmakuri
Kanta Prasad Pant
Kapil Parashar
Abhijit Manohar Patil
Abhijit Dadaso Patil
Thanuja Patil
Pradeep Kumar Atmakuri
Vishnu Preethi
Purnima Radhanath
K. Rajalakshmi
Chidananda B. Ramasetty
Anil Rana
Mukesh Rathi
Anjana Kumari Roy
Jenifer S
Vijayasankar S. Narayanan
Komal Sharma
Neelanshu Sharma
Ajay Kumar Shukla
Neeraj Singh
Viswanath Sivaramakrishnan
Basavaraj S. Deshamane
Siva Naga Harish Terli
Sonu Thomas
Tarun Kumar Tyagi
Amer Zaidi

Indonesia

Rika Astari
Miftahuddin
Hendi Yogi Prabowo
Stephanus

Ireland

Neryn Gaul
Malgorzata Jakubas
Carol-Ann Mcintyre
John McLaughlin
Ana Moreno Masa
Eanna O'Donnell
Jesús Olías Terol
Christophe Rey
Alona Sicevica
Piotr Sulek
Keith S. Taurai
Tetyana Veretelnyk
Anna Wnek

Italy

Stefano Battaglia
Giulia Faotto
Rui Liu
Greta Francesca Mantovani
Vincenzo Pitrelli

Jamaica

Ro-Yen Chin Forbes
Vera Marie E. Lindo
Rene Tamara Mitchell
Tameika-Jo Pockhai
Phueona G. Reynolds
Anthony P. Williams

Japan

Andrew Freiwald
Yasuhiko Isshiki
Yeunjung Jung
Ryan McNabb
Asuka Nakayama
Pranav Dilip Shah
Liping Wang
Jessie Chia-Jui Yu

Jordan

Asmahan Mahdi A. Alhadeethi
Abdulhakeem A. Abbood
Asad Jamil Abu Ammer
Juana Roshdi Baskharoon
Samer Faisal Talhouni
Ahmad Omer Hamad
Ahmed Hamid Jameel Al Janabi
Ahmed Khaleel Marhoon
Ban Salim Mahmood Marjan
Omar Sameer Arshid Al Bassam
Suham Hashim Taha Al Samraei
Ali Waleed D. Alabdalqadir

Kazakhstan

Yuliya Salekhova

Kenya

Esther Wanjiru Kabue
Kenneth F. Katiechi
Grace Wamahiga Muhia
Rose Wanjiku Ngeru

Kuwait

Anwar Ahmed Al Taheri
Dhaifallah Shafi Alanazi
Ahmed Ashour Mohammad
Mohamed A. A. Elbanna
Khaled Hamdy M. Hassab
Desouky Abdelaziz Nassar
Hadi Ishaq Rashed
Mohammad S Al Abdulrazzaq
Ali Akbar Sanasiri

Laos

Feng Tan

Latvia

Anna Antonova
Andis Berzins
Alla Buraja
Maija Dārzniece
Jānis Diedišķis
Linda Gulbe
Elīna Gūtmane
Mihails Hodjakovs
Natālija Ignatjeva
Ivo Ivanovs
Natalja Jesinska
Arnis Kalveršs
Victoria Kolosova
Jūlija Kondratjuka
Aleksandrs Kvedars
Karina Lindava
Jānis Lukjanskis
Inesa Luse
Kristīna Markeviča
Anna Mavļutova
Linda Mikanovska
Natalja Osipova
Tatjana Petrova
Ņina Piskunova
Mihails Porožņakovs
Aleksandrs Raizbergs
Vita Šiballo
Konstantīns Sizihs
Natalja Smirnova
Julija Strukova
Victorija Ufimceva
Inga Vevere
Jaroslavs Zamullo
Jeļena Zubale

Lebanon

Nadine M. Abou Diab
Nathalia Al Haddad
Elias Azzi
Zeina Boustani
Elie-Joe Dergham
Wissam El Hajj
Mohamad Kamel El Mekkawi
Abed El Rahman Khodor Itani
Loubna Elias Moubarak
Anis Elias Naffah
Amina Farroukh
Rawad Hammoud
Fadi Hassan Khachab
Aed Adnan Jalloul
Najah Mouhamad Khaled
Eliane F. Tanios

Lithuania

Vilius Armanavicius
Lina Gircyte-Juske
Andrius Merkelis
Zivile Slaminskaite

Luxembourg

Georges Abotchi
Anne-Claire Allain
Yuri Broodman
Carol Digioia
Abdoulaye Faye
Maxime Heckel
Mara Marangelli
Fabrice Migrenne
Cécile Moser
Vilma Ninka
Dale J. Quarry
Massimiliano Seliziato
Lofti Souilah
Jonathan Stara

Macau

Chih Hsin Chiang
Man I Leng
Linshan Luo
Lung-Chuan Su
Oi I Tam
Lok Man Wong
Wing Kwan Wong

Macedonia

Dimitar Pop-Georgiev

Malawi

Hannes Jansen van Vuren

Malaysia

Whye Hon Choy
Alvin Jiunn Kwang Han
Mohammad Amirul Bin Haspulah
Fang Jia
Mei Chen Wong
Wee Fhong Ow
Fion Nu Ting Ye

Mauritius

Yogesh Ganoo Bapjee
Madhvi Gowreesunkur Conjamalay
Veeramdeve Nem
Stephanie Emmanuelle Veerapen Chetty

Mexico

Caroline Devige
Alfredo Gutierrez-Valle
Eunice Hernandez Ramirez
Ileana Rivera Mucino
Ana Regina Rodriguez Ouchterlowny

Netherlands

Youness Aktaou
Kaylee Alblas
Timothy Ambachtsheer
Wahib Belhachmi
Can Demir
Karin Mercedes Kupzok
Kseniia Kutyreva Kutyreva
Guy Mitchell
Laura Elena Rodriguez Trillo
Elke Maria Johanna Romijnders
D.Z. Sewdihal
V. W. T. Smulders
Paulien Maria Francisca Stam
Changwei Tang
Sean Van der Hoek
Renee Natascha Hofman
Merel Eva Vermoolen
Suzanne Adriana Westra
Marieke Zandvliet

New Zealand

Jessica Channing
Andrew Christopher Crow
Marcella Fariu
Bianca Maria Fernandes
Miriam Gray
Yi Hui Hong
Andrew Johnson
Parikshit Kshirsagar
Xiao Hui Li
Sarah Meredith
Leon Schoeman
Andrew F. Simpson
Emma Stevens
Tili Talaia
Jeremy Williams
Julie Wilton

Nigeria

Joyce Adekoya
Oluwafemi Shogo Aminu
Linda Okpako Aruoture
Sechap Siman Giwa
Adegboyega Ige
Olufemi Olayiwola

Pakistan

Arbab Gohar Ghayas
Basharat Khan
Sarfaraz Ahmed
Irfan Memon
Kashif Nisar
Zishan Hasan Zaidi

Palau

Clinton Oiterong Ngemaes

Panama

Susanne Kusyk

Paraguay

Lucas Joel Lagrave Roa

Peru

Moisés Vásquez Sairitupa

Philippines

Dean Christopher S. Dimaandal
Anna Liza R. Guevarra
Samuel G. Lazaro
Arnel Venasquez Zablan

Poland

Bartłomiej Andrzejczak

Portugal

Anna Maria Adamowicz
Kamil Bartczak
Radoslaw Biniarz
Philip Bratoev
Anna Maria Brodowska
Kamil Buraczewski
Anna Chub
Lukasz Dabrowski
Horia Constantin Dragusinoiu
Paweł Dziocha
Magdalena Gaciong
Maciej Garbaczewski
Przemyslaw Goldyn
Krzysztof Harasimczuk
Urszula Jakubowska
Luiza Jarocka
Grzegorz Kapler
Julian Kiciński
Zuzanna Kot
Monika Król-Horosz
Michal Andrzej Krysinski
Jolanta Kulik
Rafał Labęcki
Piotr Lada
Piotr Lelejko
Marlena Makowka
Małgorzata Makowska
Natalia Makowska
Stefan Rafal Michalczyk
Joanna Mioduszewska
Abdul-Rauf Momodu
Karolina Opic
Elzbieta Poznanska
Rafal Sadowski
Patryk Skrzypczak
Mateusz Soćko
Radoslaw Szeller
Barbara Maria Tomczyk
Justyna Tymowska
Justyna Wasilewska
Magdalena Wilewska
Piotr Jerry Wojtasiak
Michal Wujec
Joanna Iwona Zając
Katarzyna Żelek

Puerto Rico

Mildred Garcia Rodriguez
Eva M. Marquez-Cruz
Andres Nieves Torres
Lauramir Rivera-Vélez

Qatar

Jasmin Ragasa Galacgac
Randall Vaz

Romania

Corentin Quesnel
Andreea Tampu-Ababie
Costin Tesedeanu

Russia

Evgeniya Badulina
Pavel Medvedev
Anastasiya Mokashova

Saint Lucia

Shannon Auguste
Kimberly Gillian Chassang

Saudi Arabia

Riyadh Abdullah Alnukhaylan
Najlaa Abdulrahman A. Al AlSheikh
Rana Abubaker Mahmoud Al-abed
Yousef Dhafer Al-Ahmari
Ahmed Abdualaziz Al-Baoud
Fahad Abdulkarim Aleidan
Mohsen Shahathah Al-Eniezi
Anfal Ibrahim Al-Habab
Ahmed Mohammed Madhi Al-Madhi
Alhanof Mohammed Alqahtani
Fahad M. Alsubaie
Fayez Rasheed Al-Subaie
Mazen Abdullah Alsuliman
Khaled Altawily
Faris H. Al-Yami
Hassan Ali Barasheed
Abdullah Mohammed Ezzi
Faris Hamad Al-Hattab
Nawaf Hashash Al-Enazi
Shojaa Faleh Khaled Alqureshi Alsubaie
Khaled Mutlaq Al-Otaibi
Faris Hani Tarabulsi

Serbia

Ivana Djukic

Singapore

Zhen Ling Aw
Xian Yu Boon
Olivier Brizard
Ruth Li Koon Cheng (Zhong LiJun Ruth)
Hanfeng Shaun Chia
Irene Chia (Xie Irene)
Kee Hur Choe
Yunhwa Choi
Xiao Tong Hazel Chum
Pooja Dash
Praveen Kamalnath Dewangan
Ruosen Ding
Kwai See Foo
Chandrachud Giriappa
Thian Soon Goh
Wee Hou Hay

Yuan-Li Hong
Siew Kee Hoy
Chungyi Hsu
Xihong Zavier Hu
James Nam Guan Huan
Jordan Geng Yuan Koh
Stephen Weijie Koh
Bee Suan Lee
Lay Hiong Lee
Li Ling Lee
Soon Keng Lee
Dingjian Liang
Lydia Liu
Hwei Ling Loo
Dias Malayev
Sukriti Mathur
Rishik Vijayadas Elias Menon
Ka Yin Mok
Shao Jie Ng
Win Nie Tang
Magdalene Ong
Seol Won Park
Wan Hao Keith Peh
Sudip Roy
Pradheep Kumar Sampath
Ling Ling See
Susanne Catharina Hok Shaw
Muhammad Pasha Peter Shepherd
Rohan Singh
Ping Ling Tai
Jason Wee Yong Tan
Shirly Tan
Siew Ling Jafmine Tan
Ying Xian Gregory Tan
You Leong Lawrence Teh
Pramod Tewari
Soon Kit Tham
Markus Alexander Tjoa
Julia B. Walker
Sok Mun Wan
Sin Ee Lansin Wee
Willy Wonka
Weijie Xu
Cao Yu Jie

South Africa

Kyle Bryce Chetty
Gertruida Johanna Larsson
Confidence Moliki Leboea
Thato Mohajane
Devashnee Naidu
Siziphiwe Ngxabi
Christine Patricio
Monogran Pillay

South Korea

Kye Won Ahn
Jung Hyun Choi
Sungil Heo
Yoonsung Jekal
Ji Sil Kim
Joo Young Kim
Tae Kyung Kim
Bokyung Koo
Hyounjoo Lee
Naheun Lee
Won Kyu Lee
Yu Young Lee
Yunhee Lee
Jihoon Roh
Ra Young Shon

Spain

Lorena Arroyave Casas
Juan Diez Herrero
Nora Gastaminza García
Yiti Li
Miguel Angel Ogbechie Condes
Yolanda Olivares Villegas

Sri Lanka

Inami Shanika Jayasinghe Pieris
Gamagedera M. L. Y. Bandara Ududeniya

Sudan

Ibrahim Hassan Ibrahim Osman

Swaziland

Calvin Phumlani Dlamini

Sweden

Fredrik Almquist
Alexander Eriksson
Ingrida Larsson

Switzerland

Cristina Cecilia Hidalgo Valdez
Beryl-Guy Marquis
Franco Poggi
Lina Popova
Emmanuel Stutz
Dino Zanetti

Taiwan

Lidia Au
Fang-Ching Chan
Hsiao-Ping Chan
Meng-Jia Chan
Shih-Hsu Chan
Wei-Shun Chan
Ya-Chien Chan
Bor-Dar Chang
Chao-Shen Chang
Che-Yu Chang
Chia-Chun Chang
Chia Yen Chang
Chia-Chien Chang
Chia-Fang Chang
Chia-Hao Chang
Chia-Hui Chang
Chia Ming Chang
Chih-An Chang
Chi-Jen Chang
Ching-Mei Chang
Chun Teng Chang
Chung-Wei Chang
Chun-Yao Chang
Fang-Lien Chang
Fang-Wei Chang
Feng-Chin Chang
Hsun-Yin Chang
Huang-Shan Chang
Hung-Yuan Chang
Iou-Jie Chang
Jen-Bin Chang
Jung-Chia Chang
Kai-Hui Chang
Shu Fen Chang
Lily Chang
Li-Wen Chang
Lung-Chueh Chang
Ming-Fan Chang
Pao-Chun Chang
Pei-Ching Chang
Ping-Yu Chang
Shih-Hsin Chang
Shiow-Huey Chang
Shu Hao Chang
Shuching Chang
Shu-Fang Chang
Shu-Ming Chang
Su-Fen Chang
Su-Huei Chang
Su-Hui Chang
Tingting Chang
Ting-Yu Chang
Tsung-Yang Chang
Wen Ya Chang
Ya-Hsiu Chang
Ya-Hwei Chang
Yenrong Chang
Yi-Hua Chang
Yu-Chen Chang
Yu-Chen Chang
Yu-Chuan Chang
Yueh Chin Chang
Yu-Hsuan Chang
Yu-Hua Chang
Chih Ju Chang Chien
Li Ming Chao
Sung-Shan Chao
Yee-Chin Chao
Chang-Fan Chen
Chao-Huang Chen
Cheng Ying Chen
Chen-Wen Chen
Chia Sheng Chen
Chia-Te Chen
Chia Yu Chen
Chia-Hao Chen
Chia-Hui Chen
Chiao-Lin Chen
Chieh-Jen Chen
Chien-Jung Chen
Chien-Liang Chen
Chih-Chi Chen
Chih-Ching Chen
Chin-Chu Chen
Chin-Chueh Chen
Ching Hsien Chen
Ching-Ching Chen
Ching-Min Chen
Ching-Tan Chen
Ching-Tao Chen
Chin-Yann Chen
Chiou-Liang Chen
Chiu-Feng Chen
Chi-Wen Chen
Chi-Ying Chen
Chun-Chin Chen
Chung-Cheng Chen
Chung-Yueh Chen
Chun-Lin Chen
Chun-Pin Chen
Chun-Yan Chen
Feng-Chuan Chen
Feng-Yang Chen
Fen Wei Chen
Fu-Chuan Chen
Fu-Meng Chen
Guan-Ting Chen
Guo-Xian Chen
Hsiang-Jung Chen
Hsiao-Chi Chen
Hsiao-Hui Chen
Hui Min Chen
Hui-Hsin Chen
Hui-Hua Chen
Hung Ching Chen
I-Ying Chen
Jen-Ling Chen
Jui Fen Chen
Jui-Chen Chen
Jui-Sheng Chen
Jun-Rong Chen
Chun Wei Chen
Kuan Ting Chen
Kuei-Chih Chen
Kuen-Liang Chen
Kun-Feng Chen
Kuo Hsien Chen
Kuo-Ping Chen
Li Lin Chen
Li Yu Chen
Li-Ching Chen
Li-Chu Chen
Li-Chun Chen
Liju Chen
Ling Wen Chen
Ling-Ling Chen
Mei-Hui Chen
Mei Ling Chen
Mei-Hei Chen
Mei-Hsin Chen
Mei-Jiun Chen
Mei-Ling Chen
Mei-Tui Chen
Ming-Hui Chen
Ming-Yu Chen
Mu I Chen
Nai-Chia Chen
Nai-Pi Chen
Pei Ru Chen
Pei-Tzu Chen
Po Hsuan Chen
Po-Ya Chen
Po-Yi Chen
Ruei-Huang Chen
ShangYen Chen
Sheng Li Chen
Shih-Yen Chen
Shu Chuan Chen
Shu Hsien Chen
Shu-Chen Chen
Shu-Fen Chen
Shu-Jung Chen
Shu-Min Chen
Shu-Ming Chen
Shu-Yuan Chen
Sung-Hua Chen
Szu-Chia Chen
Taixun Chen
Tsung-Hua Chen
Tzu-Wen Chen
Wan-Chi Chen
Wei-Chun Chen
Wei-Hsin Chen
Wei-Ju Chen
Wen-Chun Chen
Wen-Ling Chen
Wen-Yu Chen
Ya-Mei Chen
Yen-An Chen
Yen-Lin Chen
Yi-Fang Chen
Yi-Jin Chen
Yin-Chun Chen
Ying-Tsun Chen
Yi-Po Chen
Yi-Ting Chen
Yi Wei Chen
Yo-Wei Chen
Yu-Chen Chen
Yu-Chun Chen
Yueh Mei Chen
Yu-Fen Chen
Yu-Hsiang Chen
Yu-Ling Chen
Yu-Mei Chen
Yun-Yu Chen
Yung-Hsiang Chen
Yun-Hui Chen
Yun-Yi Chen
Yu-Shen Chen
Yu-Ting Chen
Yu-Yeh Chen
Chiao Ching Cheng
Chih-Jen Cheng
Chih-Yuan Cheng
Ching-Fen Cheng
Ching-Wen Cheng
Hsiang Ling Cheng
Hsiung-Yuan Cheng
Hsu-Kao Cheng
Jen-Hui Cheng
Li Cheng
Li-Fen Cheng
Mei-Hsiu Cheng
Ming-Chia Cheng
Nien Sun Cheng
Shu-Min Cheng
Shu-Wen Cheng
Ya-Fang Cheng
Ya-Ling Cheng
Yeh Cheng
Yen-Feng Cheng
Shuenn-Yuan Chern
Wen-Hsiung Chi
Hsiu-Chen Chiang
I-Cheng Chiang
Kuo-Tung Chiang
Li-Chuan Chiang
Ling-Chia Chiang
Mei-Hui Chiang
Nien-Chieh Chiang
Pi-Hua Chiang
Shang-Shing Chiang
Yen-Tsung Chiang
Yu-Hsin Chiang
Chih-I Chien
Hsiu Chen Chien
Yu-Ming Chien
Kuo Chih Ying
Wan-Yun Chin
Chiung-Ying Chiu
Han-Wen Chiu
Hui-Min Chiu
Lin-Lan Chiu
Mei-Hui Chiu
Sheng-Fei Chiu
Shu-Wen Chiu
Te Min Chiu
Yu-Jung Chiu
Yung-Chang Chiu
Chien-Pei Chou

Chun Yao Chou
Feng Ching Chou
Hsiang-Lin Chou
Lung-Yao Chou
Mei-Hui Chou
Ming-Yi Chou
Tzu-Lin Chou
Wen Pin Chou
Ya-Ting Chou
Ching-Wei Chu
Chiu-An Chu
Hsiu Shen Chu
Kuo-Wei Chu
Shun Ying Chu
Che-Ming Chuang
Chih-Chieh Chuang
Hsiu-Fong Chuang
Hui-Ju Chuang
Jui-Ming Chuang
Li-Yu Chuang
Mei Chen Chuang
Ming-Teh Chuang
Shu-Fen Chuang
Wen-Chin Chuang
Yu-Fen Chuang
Yu-Ning Chuang
Chun-Chih Chui
Chien-Wei Chung
Hsiao-Ling Chung
Hsien-Feng Chung
Jui-Kai Chung
Peiyao Chung
Shih-Fang Chung
Shu Hui Chung
Ya-Hui Chung
Yueh-Chun Chung
Yu-Hsiang Chung
Jia-Huei Dai
Chia-Ming Fan
Fang-Wei Fan
Tien-Hsi Fan
Chun-Kai Fang
Mei-Chu Fang
Wei Wen Fang
Ya Huei Fang
Yu-Chi Fang
Chiou-Ing Fann
Han-Kuang Feng
Mei-Chih Feng
Tsun-Hui Feng
Shi-Wei Fu
Shu-Yu Fu
Yu-Hsuan Fu
Kuo Han-Jen
Cheng Si He
Chou-Lin Ho
Guo-Hua Ho
Hsin Yi Ho
Hsing-Chen Ho
Hsin-Lin Ho
Hsuan-Kuei Ho
I-Ching Ho
Kai-Ting Ho
Kang-Yu Ho
Shu-Hui Ho
Ying Ting Ho
Chih-Kai Hou
Ya Tong Hou
Chiu-Wen Hsiang
Chih-Hui Hsiao
Chi-Ming Hsiao
Hsiang-Yen Hsiao
Ju-Yun Hsiao
Mei-Hui Hsiao
Mei-Ling Hsiao
Min Shun Hsiao
Ruei-Yi Hsiao
Shu-Fen Hsiao
Su-Chen Hsiao
Yu-Chun Hsiao
Chia-Jung Hsieh
Hsunyi Hsieh
Hung-Yu Hsieh
Kuan-Jen Hsieh
Li-Yun Hsieh
Nien-Wen Hsieh
Shu-Hui Hsieh
Ssu-Hung Hsieh
Wen Yi Hsieh
Yi-Chen Hsieh
Yi-Sheng Hsieh
Yu-Li Hsieh Yieh
Wan-Chu Hsing
Chang-Fang Hsu
Chia Hui Hsu
Chia-Pin Hsu
Chien Hung Hsu
Chih-Cheng Hsu
Chih-Hui Hsu
Ching Hsiang Hsu
Ching-Li Hsu
Chin-Wei Hsu
Chiung-Fang Hsu
Chun-Ju Hsu
Chun-Ming Hsu
Hsiang-Chih Hsu
Hsiu-Chiung Hsu
Hsiu-Ling Hsu
Huai-Yen Hsu
Hui-Ching Hsu
Hui-Lun Hsu
Hung Yuan Hsu
Jen Hsu
Jih-Tang Hsu
Kuangwei Hsu
Lu Yu Hsu
Ming Yi Hsu
Pai-Li Hsu
Pao-Fang Hsu
Sheng-Wei Hsu
Shih-Fa Hsu
Shu-Fen Hsu
Shu-Fen Hsu
Tzu-Lan Hsu
Wei-Chia Hsu
Wu Chun Hsu
Ya Han Hsu
Ya-Hsing Hsu
Ya-Ru Hsu
Yi-Yin Hsu
Yu-Chieh Hsu
Jao Hsuan
Pei-Chi Hsueh
Shu Ling Hseuh
Yi-Man Hsueh
Ying-Hung Hsueh
Lin Hsueh-Cheng
Ching Yi Hu
Chi-Yuan Hu
Jin-Fa Hu
Jo-Wei Hu
Li-Chia Hu
Shu-Ping Hu
Ta-Lung Hu
Tse Wei Hu
Wei-Ting Hu
Pin-Hung Hua
Chang-Yuan Huang
Chao-Liang Huang
Cheng Hsien Huang
Cheng-Chieh Huang
Chia-Li Huang
Chih Pin Huang
Chih-Li Huang
Chih-Wei Huang
Chin-Cheh Huang
Chin-Cheng Huang
Ching-I Huang
Chin-Wei Huang
Chin-Hui Huang
Chin-Hui Huang
Chin-Lung Huang
Chin-Ying Huang
Chi-Yuan Huang
Chun Chang Huang
Feng-Hsin Huang
Hsiao Fen Huang
Hsin-Hao Huang
Hsin-Wei Huang
Hsin-Yuan Huang
Hsiu-Fen Huang
Hsueh-E Huang
Huei-Yi Huang
Hui Chuan Huang
I-Hsien Huang
I-Ling Huang
Kuei-Fen Huang
Li-Chen Huang
Li-Ling Huang
Mei-Fang Huang
Mei-Hsueh Huang
Mu-Heng Huang
Pao-Hsia Huang
Pei Yi Huang
Pi-Shu Huang
Pi-Yin Huang
Ruo-Yun Huang
Sheng Shun Huang
Shih-An Huang
Shih-Li Huang
Shih-Pin Huang
Shih-Ping Huang
Shu-Chang Huang
Shu-Fen Huang
Shu-Hui Huang
Shu-Ling Huang
Shu-Mei Huang
Shu-Ping Huang
Su-Hwa Huang
Su-Mei Huang
Sung-Yuan Huang
Ting Nu Huang
Tsan-Yu Huang
Tsung-Huan Huang
Tzu-Chi Huang
Wei-Chun Huan
Wen-Chieh Huang
Wen-Ni Huang
Yao-Chun Huang
Yen-Hsiang Huang
Yi-Hsuan Huang
Yi-Hsuan Huang
Yi-Wen Huang
Yu Jen Huang
Yueh-Tao Huang
Yuen-Yen Huang
Yu-Hua Huang
Yu-Ting Huang
Yu-Xiang Huang
Zi-Yuan Huang
Chien Hui Hung
Chih Hsien Hung
Chih-Chan Hung
Ching-Ting Hung
Hao-Hsuan Hung
Hui-Chun Hung
Kuo Che Hung
Ling-Hui Hung
Shu Yu Hung
Shu-Ching Hung
Tien-Chi Hung
Wen-Pei Hung
Ya Hui Hung
Ya-Hui Hung
Deng-Shing Hwang
Jiann-Tsair Hwang
Shwu-Fen Jang
Vhih Yu Jao
Sin Lun Jhuang
Siang-Teng Jiang
Chiou-Ling Jou
Bao-Yueh Ju
Shoou-Bin Juang
Mei-Chu Kan
Jui-Che Kang
Chen-Chan Kao
Cheng-Chun Kao
Chih-Chieh Kao
Fang-Ko Kao
Guo Chiang Kao
Ming Chun Kao
Yi-Fan Kao
Yu Kao
Jyun-Ming Ke
Tsan-En Ke
Shu-Ping Ku
Lulu Iju Koung
Chia-Chu Kuan
Chun-Lien Kuan
Yen-Li Kung
Yi-Fen Kung
Yu-Kai Kung
Yu-Shih Kung
Chia-Chun Kuo
Chun-Yi Kuo
Kun-Lin Kuo
Li-Jen Kuo
Ming Fang Kuo
Ting-Shur Kuo
Tsung-Hao Kuo
Tzu-Chieh Kuo
Wei-Chun Kuo
Wen-Chun Kuo
Chun-Hung Lai
Hsin-Yu Lai
Hsueh-Ling Lai
Kuan-Hao Lai
Kuan-Ju Lai
Mei-Ling Lai
Ming-Yuan Lai
Shu-Chen Lai
Wen-Ling Lai
Ya-Hsueh Lai
Yi Jung Lai
Yuan-Sheng Lai
Yu-Jung Lai
Yung-Chang Lai
Bo-Dung Lan
Ching-Ju Lan
Shih-Fang Lan
Wu-Wen Lan
Ying-Yi Lan
Cheng-Hsien LEe
Chien-Chih Lee
Chih-Chieh Lee
Chih-Hung Lee
Ching-Yun Lee
Feng-Hsien Lee
Feng-Ying Lee
Hsiao-Wen Lee
Hsin-Yi Lee
Hua Wen Lee
Hui-Hua Lee
I-Ting Lee
Kuan-Ying Lee
May-Ying Lee
Mei-Chu Lee
Mei-Fen Lee
Mei-Hua Lee
Mei-Hui Lee
Mei-Lin Lee
Mei-Yin Lee
Ni Lee
Pi-Ju Lee
Shui-Chiao Lee
Su-Fen Lee
Sze Ying Lee
Tsui-Wan Lee
Tung Sheng Lee
Ya Hui Lee
Ya-Szu Lee
Yi Shan Lee
Yi Yun Lee
Ying-Liang Lee
Yun Sui Lee
Chen-Ying Li
Ching Hsiang Li
Chun-Mei Li
Hui Chun Li
Jyun-Long Li
Pei Yu Li
Ting-Yi Li
Tsunghan Li
Yen Ching Li
Yu-Lan Li
Horng Dar Lian
Yeh-Kang Liang
Yu-Jen Liang
Chieh-Ju Liao
Ching-Chin Liao
Chin-Ming Liao
Feng-Hui Liao
Jia-Ling Liao
Jing-Qi Liao
Pei-Ju Liao
Pei Ling Liao
Pei Ling Liao
Shu-Chen Liao
Shu-Yu Liao
Tiao Sheng Liao
Wan-Hui Liao
Yen-Yi Liao
Yi-Chia Liao
Yu-Mei Liao
Chia-Yung Liaw
Bo-Shiun Lien
Chih-Yuan Lien
Tsao-Shun Lien
Chao Ju Lin

ACAMS® | Chapters

BUILD YOUR LOCAL NETWORK

The ACAMS Chapter Development Program aims to focus the association's international efforts in anti-money laundering education and training at a local level. Chapters foster professional relationships and provide local forums for discussion around region-specific issues.

FIND A LOCAL ACAMS CHAPTER NEAR YOU OR START ONE TODAY!

WWW.ACAMS.ORG/CHAPTERS | CHAPTERS@ACAMS.ORG

Chao-Cheng Lin
Chao-Kuo Lin
Cheng-Tang Lin
Chia-Cheng Lin
Chia-Chun Lin
Chia-Hui Lin
Chiao-Wen Lin
Chiao-Yu Lin
Chia-Sheng Lin
Chien-Chih Lin
Chien-Hung Lin
Chih-Jou Lin
Chih-Heng Lin
Chih-Ling Lin
Chih-Wen Lin
Chi-Ming Lin
Chin-Da Lin
Ching Chih Lin
Ching-Yi Lin
Chiu-Ling Lin
Chiung-Yi Lin
Chun-Ying Lin
Chun Ying Lin
Chun-Chieh Lin
Chun-Hung Lin
Chun-Te Lin
Chun-Yu Lin
Fang-Ju Lin
Hai-Li Lin
Hsaing-Ching Lin
Hsin Hua Lin
Hsin-Yu Lin
Hsiu-Chuan Lin
Hui-Hsiang Lin
Hui-Min Lin
Hung-Yen Lin
I Chieh Lin
I-Ling Lin
Jin-Jr Lin
Ju-Hsiang Lin
Ju-Ya Lin
Kun-Ying Lin
Lee-Hsuan Lin
Li-Jung Lin
Li-Kuan Lin
Li-Mei Lin
Li-Na Lin
Ling-Hwa Lin
Lo-Sung Lin
May Ju Lin
May-Yeh Lin
Mei-Hui Lin
Mei-Hung Lin
Mei-Hung Lin
Mei-Ling Lin
Miao-Ling Lin
Pei-Yao Lin
Po-Yi Lin
Sheng-Te Lin
Shiang-Yuan Lin
Shi-Da Lin
Shih-Hsuan Lin
Shih-Jung Lin
Shu-Feng Lin
Shu-Hsien Lin
Shu-Hsin Lin
Shu-Hui Lin
Shwu Fen Lin
Tsung Yu Lin
Tsung-Ching Lin
Uei-Jyh Lin
Wan-Chen Lin
Wei-Chi Lin
Wei-Ju Lin
Wen-Chuan Lin
Wen-Yi Lin
Ya-Ting Lin
Yen-Nien Lin
Yi Chia Lin
Yi Hua Lin
Yi Mei Lin
Yi-Hsin Lin
Yihsun Lin
Yijun Lin
You Yeh Lin
Yu Chuan Lin
Yu-Chen Lin
Yu-Cheng Lin
Yu-Cheng Lin
Yu-Chuan Lin
Yu-Fang Lin
Yu-Mei Lin
Yun-Ching Lin
Yun-Chiueh Lin
Yung-Ju Lin
Yun-Ju Lin
Yu-Su Lin
Yu-Ying Lin
Lie-Yea Liou
Chia Ko Liu
Chia-Ching Liu
Chih-Chen Liu
En-Ting Liu
Hsiao-Lin Liu
Hua-Chen Liu
I-Tzu Liu
Keng-Hao Liu
Li Fang Liu
Mei-Ju Liu
Mei-Yu Liu
Shao-Chieh Liu
Shiang-Lin Liu
Shu Hui Liu
Shu Hui Liu
Shu Ning Liu
Ting-Chun Liu
Tsai-Chin Liu
Tsui Ting Liu
Tsui-Hua Liu
Wen-Ching Liu
Wen-Feng Liu
Yao Tsung Liu
Ying-Chi Liu
Yi-Ting Liu
Yu-Jui Liu
Yun-Chien Liu
Yun-Chun Liu
Chiao Sen Lo
Chiu-Yueh Lo
Hsiao-Yen Lo
Hung-Lin Lo
Peilin Lo
Yi-Fan Lo
Yu-Ching Lo
Chih-Hung Lo
Chun-Mien Lu
Jung-Chuan Lu
Lin-Jeng Lu
Li-Wen Lu
Pao-Chun Lu
Ping Yu Lu
Wei-Tsung Lu
Yan Fen Lu
Yi-Ning Lu
Yu-Chien Lu
Yuling Lung
Shu-Chen Luo
Huei-Ling Ma
Tzu-Ching Ma
Tsu-An Mao
Wu-Yang Mao
Chin-Cheng Ni
Yueh-Yen Ning
Chuehhua O
Chiu-Yin Ou
Hsueh Fen Ou
Hsiao-Chun Ou Yang
Meng Chun Ou Yang
Chin Chia Pai
Fang-Jung Pai
Min-Hua Pai
Chao-Chiun Pan
Chieh-Min Pan
Shih-Huang Pan
Chih-Yung Pao
Chih Wei Peng
Chun-Ming Peng
Hsin-Ling Peng
Huey-Chuan Peng
Kuan-Hao Peng
Mei-Ching Peng
Ming-Yuan Peng
Sheng-Hsiang Peng
Yu-Feng Peng
Chung-Jui Shen
Yueh-Chu Shen
Shu Hong Shiau
Shian-Yi Shie
Ching-Yu Shieh
Cheng-Yi Shih
Chi-Chin Shih
Chih-Cheng Shih
Ching-Wen Shih
HsiaoChun Shih
Hua-Yin Shih
Mei-Ming Shih
Shun-Liang Shih
Tung Hsin Shih
Yu-Tsung Shih
Huang Shih-Yin
Chang-Tai Shiung
Kuo-Hsin Shu
Wang Shu-Cheng
Wan-Ting Shueh
Chuan-Hui Su
Hsiang-Yu Su
Hsi-Hsun Su
Hsin Yu Su
Hsin-Yuan Su
Hsueh-Lien Su
Mei-Ying Su
Yi Pei Su
Yu Chia Su
Yu Chih Su
Chia-Man Sun
Chi-Jen Sun
Chuan-Chuan Sun
Chung-An Sun
Hsiao-Hsuan Sun
Shu Mei Sun
Ya-Chuan Sun
Hsin-Chieh Sung
Meng-Jen Sung
Shun-Chang Sung
Yi-Siang Tang
I-Change Tasi
Chan-Sen Teng
Tsai-Hsien Teng
Li-Chen Tien
Hui-Mei Ting
Chun-Shing Tong
Bor Yi Tsai
Chang-Fa Tsai
Chang-Pang Tsai
Cheng-Tsung Tsai
Cheng-Ying Tsai
Chia Hong Tsai
Chien-Ping Tsai
Chi-Huang Tsai
Chi-Jen Tsai
Ching-An Tsai
Ching-Fei Tsai
Ching-Yu Tsai
Chiu-I Tsai
Chuan-Chuan Tsai
Chung Yao Tsai
Hung Shen Tsai
Hsiang-Hung Tsai
Hsiao-Hui Tsai
Hsing-Fen Tsai
Jin Ling Tsai
Jung-Wen Tsai
Kao Ming Tsai
Li-Hsun Tsai
Meng-Hsueh Tsai
Min-Hsuan Tsai
Pei-Chen Tsai
Peiling Tsai
Shih-Wen Tsai
Shu-Ling Tsai
Shun-Te Tsai
Szu-Hui Tsai
Tien-Yung Tsai
Tsung Cheng Tsai
Tsung Yu Tsai
Tsung-Han Tsai
Wei-Lun Tsai
Wen Sheng Tsai
Ya Wen Tsai
Yi-Chen Tsai
Yi-Tad Tsai
Yueh-Hsia Tsai
Yung-Ching Tsai
Yun-Jui Tsai
Yu-Ting Tsai
Hui An Tsang
Chin-Yun Tsao
Hsien-Ching Tsao
Chiao-Wen Tseng
Chih-Ming Tseng
Chun-Ching Tseng
Hsiang-Ting Tseng
Hsing-Yi Tseng
I-Hua Tseng
Li-Ling Tseng
Shu-Mei Tseng
Su-Ting Tseng
Ting-Yu Tseng
Yu Chuan Tseng
Yu-Yi Tseng
Chih Hsiang Tu
Chih Hsien Tu
Lai-Hao Tu
Shu-Chin Tu
Shu-Feng Tu
Wei-Han Tu
Yu-Chen Tu
Yun-Chia Tu
Chi Ting Tung
Chi-Chieh Tung
Hsing His Tung
Shih-Jung Tung
Yu Ming Tung
Shwu-Huey Tzeng
Yi-Mei Tzou
Cheng-Lang Wang
Cheng-Ta Wang
Chia-Nung Wang
Chien-Chia Wang
Chi Fang Wang
Chih-Chao Wang
Chih-Chun Wang
Ching-Chih Wang
Ching-Hui Wang
Ching-Wen Wang
Chiu-Cheng Wang
Chiung-Yu Wang
Chuan Yao Wang
Chun-Fa Wang
Chun-Fang Wang
Fang Pei Wang
Hao-Jen Wang
Ho-Jung Wang
Hsiang-Min Wang
Hsuan-Hsin Wang
Huei-Lan Wang
Hui-Chen Wang
Hui-Ching Wang
Huo-Yen Wang
Jui-Feng Wang
Jui-Te Wang
Kai-Ying Wang
Kai-Yu Wang
Kuo-Shu Wang
Li-Fen Wang
Li-Yueh Wang
Mei Jyh Wang
Mei-Yueh Wang
Pao-Juei Wang
Pei-Shan Wang
Pei-Ying Wang
Ruo Yin Wang
Shih-Man Wang
Shih-Yu Wang
Su-O Wang
Tai-Chun Wang
Tair-Der Wang
Tsuei-Shing Wang
Tung-Ping Wang
Tyng-Jen Wang
Tzu Shen Wang
Wu-Huang Wang
Yen Hsiang Wang
Yi Fen Wang
Yi Hua Wang
Yi Jhen Wang
Yi-Ju Wang
Yu-Ju Wang
Yun-Fu Wang
Chun-Hsia Wei

Miao Hsiu Wei
Shu-Yun Wei
Yi Ju Wei
Chia-Yu Wen
Chiu-Ping Wen
Jyh Ching Wen
Yan-Ru Wen
Cheng-Huang Weng
Chia-Chun Weng
Chieh-Yu Weng
Chih Chin Weng
Tien-Lung Weng
Tzu-Chi Wong
Chao-Jung Wu
Charng-Renn Wu
Chiang-Yin Wu
Chi-Mei Wu
Ching Miao Wu
Chuan-Feng Wu
Chun-Heng Wu
Chun-Hui Wu
Chun-Kuei Wu
Fen-Ying Wu
Han-Chin Wu
Han-Chin Wu
Hsi Hua Wu
Hsiao-Chien Wu
Hsin-Ling Wu
Hsiu Lien Wu
Hsiu-Chuan Wu
Hsiu-Tan Wu
Hsueh-Chi Wu
Hui-Ching Wu
Hui-Chun Wu
Hwang-Chou Wu
Jia-Chiann Wu
Kuan-Chen Wu
Li-Min Wu
Meilin Wu
Ming Huang Wu
Pei Hsuan Wu
Pei-Chun Wu
Pei-Guei Wu
Ping-Hsuan Wu
Shiow-Ling Wu
Shu Ching Wu
Su Chin Wu
Szu-Hsien Wu
Tung Lin Wu
Tung-Feng Wu
Tze Wei Wu
Tzu-Yen Wu
Wan-Ju Wu
Ying-Hui Wu
Yu Chun Wu
Yu-Fen Wu
Shou-Pang Yan
Chia Ming Yang
Chia-Cheng Yang
Chien-Hui Yang
Chi-Ming Yang
Chin-Chieh Yang
Chun-Sung Yang
Hsiu-Ju Yang
Hui Hsiang Yang
Hui-Hsin Yang
Chung Kang Yang
Jhih-Ciang Yang
Liang-Jia Yang
Meng-Ling Yang
Sheng-Tine Yang
Shuhua Yang
Siou-Huei Yang
Wan-Ju Yang
Ya Hsuan Yang
Ya-Hui Yang
Yi Hang Yang
Yi-Hui Yang
Ying-Tzu Yang
Yueh-Lin Yang
Yuh-Lin Yang
Zhen Ming Yao
Bo-Gang Yeh
Chao-Lin Yeh
Se-Ying Yeh
Shu-Hua Yeh
Tung-Ming Yeh
Wen-Kuei Yeh
Yangming Yeh
Yi-Hua Yeh
Yin-Hao Yeh
Hsiu-Chen Yen
Hsuehju Yen
Pin-Chu Yen
Shih-Yu Yen
Pi-Chieh You
Chao-Yi Yu
Chen Yi Yu
Cheng Lin Yu
Chia-Wen Yu
Chia-Yen Yu
Chih-Chao Yu
Ching-Yi Yu
Hsueh-Hua Yu
Li-Chen Yu
Mei-Hui Yu
Mei-Yun Yu
Shih-Yin Yu
Ying-Chieh Yu
Yu-Ting Yu
Yu-Tsai Yu
Tai-Chin Yuan
Jia Feng Yueh
Wei-Ting Zhang

Thailand

Benjawan Keirtjaroonsiri

Trinidad and Tobago

Robby Bhola
Anthony Andrew Cartwright
Raquel Clarke
Barbara Roxanne Gillian Forde
Virginia Hillaire-Brown
Suein Law
Joanne Webb

Turkey

Murat Ozturk

Turks and Caicos Islands

Brook Capron

Uganda

Mark Samuel Luswata

Ukraine

Mykyta Bieliakov
Svitlana Golubchik
Andrey Serdiuk

United Arab Emirates

Marwa Waleed Akkaoui
Ahmed Burhan Al Hasan
Mahmoud Al Nawati
Tahmina Asimova
Christopher Joaquin Barroga
Narathota Hewage Thilini S. Benedict
Laura C. Berche-Sigrist
Kapila Bhgaya Chandrapala
Sui Kheng Cheong
Payal Bhatia Chopra
Kinjal Hardik Chothani
Muhammad Adnan Danish
Jyoti Das
Elie El Khoury
Punit Kumar Jain
Sajan Kishore
Aziz Mahdi
Ali Makki
Nadeem Maniar
Safiya
Madmood Noufal K. M.
Veronica Oryem
Ammini P
Neeta Vijendra Pai
Pawan Randev
Beatriz Rodriguez Silveira
Feroz Ali Sajjad
Samah Salib
Srinivasan Sampathvenkat
Amena Shahbaz
Vinaya Shetty
Mahvash Shoaib
Seena Syamasundaran
Zeena Thapa
Beste Ulga Sutter
Judith Wason
Jun Xu
Rami Hani Farag Zaki

United Kingdom

Fosua Adjepong-Amankwah
Olakunle Samuel Akande
Oluwakayode Alli
Victoria Anderson
Emily Arries
Russol Akil Eraibi Bashagha
Derya Bekar
Amal Benallou
Kamal Kpur Biring
Melissa Buray
Nicholas Cerutti
Chika Chukwujekwu
Emma K. Cory
Cedric d'Albis
Raisa Das
Arindam Dasgupta
Elena Doblado Patiño
John Dunlop
Graham J. Edwards
Margrit R. Frequin
Daniel Fuller
Elchin Gadimli
Fan Gao
Euan Gregory
James Hammerton
Iva Nikolaeva Ivanova
Jose Jaramillo
Diane Katumba
Amandeep K. Khunkhun
Vinu Krishnan
Anne Li
Richard Evan Lloyd
Ahmed Madjaji
Begona Millos-Alfeiran
Emma Mills
Stuart A. Milne
Anchal Mohan
Jordan Moxey
Nikhath Mukhtar
Kristina Nelson
Emmanuelle Neuts
Andrew Y. K. Ng
Akinlayo Ogunribido
Christian Nwabueze Onowu
Kleber Palone
Mong Peng Lim
Mark Philpott
Olegs Pilipcovs
S Premkumar
Alexander Procopiou
Supriya Raghuthaman
Eve Rahmani
Nerea Ruiz Rodriguez
Sadiq Ajibola Salami
Florian Schwan
Zainab Shode
Liliya Nikolaeva Simova
Shana Sivakumar
Kim Smith
Vicky Ann Smith
Dominic Andrew Squires
Elena Sukhanova
Samson Taiwo
Meral Unlu
Alise Viba
Wenqi Wu

United States

Andrew J. Abdalla
Sundeep Addanki
John W. Adkisson
David Agayev
Andrea Agnew
Zachary Agudelo
Adam Ahmad
Ingie Ahmad
Subehee Shahrin Ahmed
Daniel Aldama
Nasreen Ali
Diana M. Allen
Heather Anne Allen
Julie A. Allen
Chris Alme
Isa Alvarez
Peter Ambery
Michael Amrine
Jene Anders
Josimari Andrade
Andrew Araujo
Wahidullah Arefi
Javier Gonzalo Arispe
Ana Armas
Debra Armour
Brooke Leigh Armstrong
Harpreet Arora
Eric Arthur
James M. Ash
Gaylene M. Ashby
Naim Askar
Samson Au
Aleksejs Babics
Jared Michael Baer
Alidad Bahrami
Bessima Bahri
Lydia Bailey
Ravinder Kumar Bajaj
Dominick Balistreri
John Scott Ballman Jr.
Kamal Kant Bansal
Mike Barbato
Robert Baron
Olivia Barron
Maya Barrow
Nilesh Baxi
Crystal Nicole Bean
Eric J. Beck
Sheree D. Beck
Laura Becker
Leslie Bedwell
Richard D. Bendekovic
Neil Benedict
Melissa Benjamin
Luis Berrios
Michael Best
Jack R. Beyer
Stephanie Bier
Joann Birlet
Eugene Bleier
Douglas A. Bolton
Mary Bonsby-Brock
Ashley N. Bouchard
Matthew W. Bower
CaDonna Grant Bratton
Jeffrey R. Braunger
Erin Brentin
Meisha N. Brisbane
Alex C. Brito
Rebecca Broadwell
Asher Brown
Sonya R. Brown
Laura Brunelli
Jocelyn J. Bruton
Brunel Brutus
Kristi Ann Buckalew
Erica L. Burakowski

Grace Burns
Veronica Byrnes
Enny Cabrera
Lawrence Louis Calderone
Frances Joy A. Caldwell
Olga A. Caltzontzint
Eugenio Alonso Calzada
Kerasha Campbell
Claudia A. Canada
Rick David Cantu
Brian R. Cappadona
Maegen Carlson
Robert M. Carlson
Susan A. Carrano
Emily Louise Case
Benjamin Cash
William C. Cassano
Jeremiah Champ
Chile (Jeffrey) Chan
Sarah Chang
Rakeem Andre Chapman
Zhen Chen
Zhiqiang Chen
Suset Cheong
Bonnie Cheung
Natalie N. Christie
Mandy Chung
YuJin Chung
Mikhail Chykiliov
Taylar Cobb
Vilma Y. Coffman
Matthew James Cole
Clifford Coles
Ryan E. Collins
Genene N. Colter
Rhina Compton
Trevor Concannon
Michelle M. Connelly
Brooke Contreras
Francy Contreras Mora
Keshia Naomi Cooper
Chrystal Corazza
Edwin Coronel
Kelly Cossaboon
Peter Crawford
Nathan Daniel Cromley
Jiayuan Cui
Hawa Curry
Luke Cushing
Michael J. Czosnyka
Caterina Da Silva
Hrishikesh Hiralal Daga
Laura Darias
Wesley Darr
Yolanda Davie
Albert de la Huerta
Gina M. Deckard
Itzel del Castillo
Nicole Del Rosario
Madelaine DeLuca
Leslie P. DeMarco
Anna Welsh Dempsey
Rachelle A. Derr
Melissa Diaz
Christopher Allbright Dillon
Marc W. Dionne
Shikha Dogra
Monique Doherty
James P. Downing
Susan Drayden
Ana Lily Duenas Arias
Elizabeth Chang Dunning
Helena Duran
Shane Dwyer
Brian H. Dyer
Eric Dziengelski
Christa Edwards
Mohamed Eldak
Miguel G. Elliott
Danielle M. Emhoff
Roosevelt Enajekpo
Michele M. England
Pamela J. Englert
Aileen Rodriguez
Alexandra Epstein
Martin A. Espinal
Daniela Espinel
Sheila Eyler
Richard Jason Fairbanks
Adrianna Farmer
Charles Farr
Peter Feher
Alana Feibus
Silvia Feliciano
Karen Michelle Feng
Steven Ferrara
Crystle L. Fielder
Michel E. Fileto
Frank Finizia
Benjamin Fischer
Jeffrey R. Flora
Michael Foley
Jannon M. Forsythe
Kelli D. Foy
Pete Francis
Tonya Fraser
Alicia Frazette
Brian Adam Frederick
Sean J. Friday
Ethan Gagne
Anthony D. Gaipa
Eric Michael Gallardo
Katherine Leova Galvan- Rodriguez
Jannick Ganz
Jennifer R. Garcia
Lauren Elizabeth Garcia
Pedro Garcia
Peter A. Garcia
Veronica M. Champsaur
Diogo Garnecho
Pamela Ann Garner
Sophia Geier
Christine A. Gibson
Tammy R. Gilleland Bangs
Travis R. Gillispie
Mitchell Guinn Glazier
Daniel J. Gloria
Brian Keith Glotzbach II
Tyler Gobin
Amanda Godt
Ivette Goizueta-Mendes
Janexis Cruz Goldberg
Wayne Gonzales
Stephanie Gonzalez
Philip W. Goode III
Amber Goodrich
Pratish P. Govind
Nandakumar Govindaraj
Kimberly D. Gowens
Eric T. Graf
Gina L. Green
Matthew Greene
Nicholas R. Griffin
Ginnie Suzanne Griffith
Benjamin Gross
Robert Lawrence Grosshart
Anna Grover
Marisa B. Guerra
Dong Kun Guo
Stephanie Jane Haan
Kathy Hadrava
Amanda J. Hale
Thomas E. Hale
Stephen Haley
Kimberly Halkett
Patrina Chongchit Hanesana
Evan L. Hankins
Heather R. Hansen
Justine Perry Hansen
Yaksheshwar Ram Hansraj
Kaitlin M. Harp
Shannon M. Harrison
Adrianne R. Hart
Lori Hartings
Brianna Hartley
Lisa Hartsell
Richard D. Haskins
Jennifer E. Haycook
Olive Healy
Nancy Hedges
Samantha Heim
Karen Anne Henderson
Jack S. Henneberry
Moravia Henry
Karen Francesca Hermosa
Monique Hernandez
Robert Brennan Heuchling
Yaffi Hilili
Kathy Hill
James Hitchcock
Jason K. Hitchcock
Betsy Hocutt
Greg Hofland
Lori L. Holmgreen
Samuel Holt
Irene Hyepom Hong
Steve Hong
Kali T. Howard
Jerome Howe
Valbona Hoxha
Aaron Hrach
Nicole J. Hroncich
Ying-Chi Huang
Frank D. Huber
Lara Huffman
Kerry Humphreys
Faneeza R. Ibrahim
Stephanie A. Ijoma
Sandy Y. Im
Donald Ingrasselino, Jr.
Christine Anne Intravaia
Modupe Irerua
Megan A. Isherwood
Megan A. Istre
Matthew Iverson
Jyoti Sekhar Iyer
Wilfried Jackson
Brook E. Jacobs
Tracy A. Jarvis
Molly Michelle Jeltema
Deborah Jimenez-Garcia
Heather N. Johnson
Jeffrey Johnson
Shannon L. Johnson
Stephanie L. Johnson
Quanesha Johnson-Pearce
Brian Johnston
Dawn Johnstonbaugh
Olivette Carol Jolly
Alexander Sherman Jones
Alexandra Jones
Jackie J. Jones
Kevin M. Jones
Sarah Anne Kathlyn Jones
Stephen C. Jordan
Byoungjoon Jun
Thomas Kaleda
Andrew A. Kampe
James Kang
Noam Katz
Audrey M. Kauffman
Ali Kazmi
Kelly Keffeler
Deborah Keifer
Jonathan Kelii
Laszlo J. Kemenczes
Stephanie Keo
Brian Keogh
Karen M. Kett
Bhumika Khandelwal
Carole P. Kibler
Alison L. Kim
Sang-won Kim
Stephen C. Kimmel
Andrew J. King
Arla King
Brandon King
Jesse Kingdon
Christina Lyons Kirby
Rich Kismer
Edward Kiss
Amy Klebesadel
Lisa S. Knoll
Carla J. Knudsen
Eliana Arend Kolenovic
Thomas J. Koller
Brandi Kollross
Harmiti Kondal-Narwal
Angela M. Koutsouris
Stephanie M. Krug
Lisa M. Krysmalski
Arun Kumar
Jessica Kump
Blake Scott Labrato
Jacob LaFlamme
Anam Lalani
Anita Lam
Farah Lamarre
Jarrod M. Landers
Stacy Michelle Langston
Adam J. LaPorte
Linda C. Large
Reed Parker Larsen
Jamie L. Laspia
Gerardo Lazaro
Brent A. LeBlanc
Christine Lee
Jackie Y. Lee
Seung Goo Lee
Ye Eun Kristy Lee
Laura A. Leister
Vincent Leo III
Morenike Entiuno Leon
Tamar C. Leon
Raymond Leong
Gabriele Leonhard
Alaina Marie Lester
Stacy A. Levine
Michael Lewchuk
Renisha L. Lewinson
Jacki Lewy
Jiaoyan Li
Jiyang Li
Shaochang Li
Yu-Hsien Liao
Ta Jung Lien
Jordan Lipschutz
Paul M. Litchenberg
Eric Liu
Siyang X (Stacy) Liu
Zhenhua Liu
Heather A Lockard
Janice Loo
Jenniffer D. Lopez
Marlon Lord
Lauren Lostritto
Frank Louigarde
Andrea Lozano
Samuel S. Luff
Debbie Lundgren
Dana Mitchell Lutenegger
Jeffrey A. Lyttle
Rod Machado
Rachel Machinton
Madhavi Latha Madduri
Pedro J. Madrigal
Anthony M. Maestas
Melissa Mai
Andrea Mainardi
Diego Malagon
Jennifer M. Malich
Gian Carlo Mapoy
Johanna Martinez
Jessica L. Marusa
Vivian Mason
Laura Maxwell
Marcus Mayfield
Amy K. McCane
Christine McCombs
Alyssa R. McDaniel
Dena McDonald
Marthe McDonald
Susan McDonald
Rodney McElrath
Sylvia A. McGaughey

Gregory McGinley
Erica McGinnis
Matthew McNeill
Jeanne B. McPherson
Jaclyn Bautista Meador
Rebecca Medcalf
Stephen P. Meduri
Ethan Meister
Michael Mekaru
Meg E. Merrill
Christopher C. Metcalf
Marcin Micek
Edita Mielkiene
Bynum Craig Miller
Danielle A. Miller
John R. Miller
Jeffrey Milton
Sean Milton
Gookhi Min
Danielle J. Miyagishima
Kenneth Mize
Mary Helen Mizzell
Joshua B. Mnich
Samantha L. Moffie
Mahera Momin
Rebecca Mondonedo
Brittany Mae Montanye
Jason R. Moorhead
Gholamreza Moradi
Vicente Moran
Bethany R. Morey
Cindy Motz
Marla Mullen
Andrea Michelle Munoz
Christopher Muros
Jami Myers
Angelo Naccarato
Vani Narra
James Casimir Naylor
Daniel Nelson
Thomas Nerad
Bernard Nery
Kenneth Newman
Matthew Newman
Ifeanyi Nnoham
Jade E. Nobles
Jordan Norris
Igal Nosovicki
Koffi K. Nsougan
Tracy A. Nystrom
Todd A. Oberhausen
Jenna O'Brien
Terence H. O'Brien
Patricia O'Connell
Meaghan O'Donnell
Catherine Lee Ogrodnik
Raymond C. Ohakwe
Sarah Osmani
Braeden J. Oswald
Rainier Nirza Pabuna
Veronica Pagenel Espaillat
Francesc Xavier Pallas Saladie
Jennifer Papenhagen
Hyunwook Park
Leah D. Park
Cassie Parncutt
Stephanie Desiree Partin
Colleen Paschal
Carolynn Paschall
Neha Patkar
Peter Patrikios
Damon Paxton
Ali Pearson
Kevin Gregory Pearson
Megan M. Peck
Idealda Perez
Robert W. Perez
Braden M. Perry
Hanh Pham
Trinh Pham
Carlos Pierre
Krishna Pillai
Maria Gabriela Pimentel Avila
Ilaria Pirocchi
Brenda Nohemy Plascencia
Angela S. Pointer
Anthony Pontosky
Christina Poplow
Danielle R. Poritz
Lorenzo A. Porras
Pamela Poulos
Satya Prakash
Timothy Alan Prevost
Jennifer A. Price
Malia Christine Price-Morris
Tudor Prisneac
Irina Pritchett
Lee R. Prowell
Vijay B. Puram
Wael Qahoush
Kendall R. Quarles
Sara Quintana
Omar Emlio Quinteros
Alison Rabbiner
Shridevi Rajkumar
Andrew Ramos
Amanda L. Raper
Donald P. Rappaport
Mahsa Rast
Diana Ravagnan
Chamundeswari Reddipalle
Christopher Reginald White
Colin B. Reid
Shara L. Reinfurt
Justin M. Remschneider
Rebecca Kathleen Reynolds
Jessica Nicolle Ghieh Ribeiro
Christina Richardson
Enrique Fernando Riguero
Mitzia Rios
Mirjana Ristic
Bernise Rivera
Michael A. Rivera
Polly A. Roberts
Sarah N. Roberts
William Roberts
Dorina Rocha
Michael J. Rodriguez
Sean Bradley Rogers
Victor Romero
Jacob Romoser
Jeff Rose
Jeremy Rosenberg
Brent T. Ross
Samuel Joseph Ross
Louis J. Rossi, Jr.
John Mark Roszkowski
Gina Roy-Dykes
Alison S. Rozbruch
Yelena Rubiner
Laura Rudolphi
Adrian E. Ruiz
Annette Runions
William M. Rusch
Laura Irane Rusignola
Dowse Bradwell Rustin, IV
Natalie H. Sadon
Nitin Sagar
Jacqueline Herrera Salais
Timothy J. Saldibar
Lila Salemi
Roxanne Saltijeral
Michael Esteban Sanchez
Paola Sanchez Torres
Daniel Sanderson
Christina Anne Santino
Jamie Sara Blistein
Justin Sarmento
Sharon M. Saverse
Melodie A. Schilling
Adam E. Schroeder
Saptarshi Sen
Thirunavukkarasu Sethuraman
Prashant R. Shah
Vikram Shah
Allison Sheckells
Si Shen
Max Sherman
Thomas Shimada
Najela Shokoor
Austin M. Shoup
Mansoor Siddiqui
Jairo Silva
Trevor Simmons
Lauren Elizabeth Sinacola
Beverly Sines
Judith Slowly
Jason R. Smith
Allison Snyder
Bryant Snyder
Ivan Solotov
Kimi Spall
Richard Randolph Spilmann
Matthew Spivack
Jonathan A. Stamm
Jennifer J. Stamper
Sharra Stapleton
Jamie Lynn Steinberg
Ara Stepanyan
George Stewart
Kari Stowe
Callaye Strauss
David Brian Strife
Karel Suarez
Szymon G. Sudol
Aizhan Suigenbayeva
Rajan Sundaram
Karen Sylvester
Jonathan Taber
Brian Tam
Sandeep Tarayil
Preeti Tata
Amanda L. Taylor
Christopher W. Taylor
William Tejada
Joshua Templeton
Pramod Narayan Tewari
Ronald Thibodeaux
Craig D. Thomas
Stephen Ray Thompson
David A. Trevino
Tara Troiano
Jean Turenne
Heather L. Turner
Jamie Ulbrich
Jeffrey S. Vales
Sherezade Valette Seijas
Daniel Abraham Grant Vallejo
Eric Van Dorn
Eric VanHorn II
Ysabel Vargas
Rebecca Lynne Vaughn
Susie Vendrell
Nefertiti N. Vernon
Gregory Vertule
Guillermo Villagrana
Eric Boyd Vogeler
Sean Voisin
Okechuku Wachuku
T'Pring N. Wade
Elaine Walters
Walter Wang
Ying-Chun Wang
Jackie Ward
Lara Valenti Ward
E. Catherine Warren
Heather A. Watson
Adam Weber
Elizabeth Weber
Hillary C. Weinberg
Jonathan Weiss
Katherine Wenger
Amanda L. West
Caleb White
Allyson M. Wiblemo
Nathan Wiest
Deborah Lynn Williams
Tyler J. Wilson-Menting
Jason Wingo
Allison N. Wirth
Kieran M. Wittbold
Sara Wolf
Matthew Wong
Grace Woo
Han Seung (Peter) Woo
Aja Woods
Corwin Wyatt
Sophie (Ruifeng) Xu
Tiffany Yamini
Xitong Yan
Hui-Tzu Yang
David Matthew Yates
Leanna Yee
Wawa Yin
Mark J. Yost
Jin Kook You
Farrag N. Yousef
Annie Yu
Robin Zakzeski
Francisco J. Zendejas
Wenbo Zhang
Yan Zhang
Dong Zheng
Harry Zhou
Lucy Zhu
Yizhe (Julia) Zhuo
Qinnan Audrey Zwick

Vietnam

Thi Phuong Linh Nguyen
Thi Tuyet Mai Pham

Zimbabwe

Webster Madera
Tonderayi Makoni
Muhammad Umar

fenergo:

DIGITALIZING TO MANAGE REGULATORY CHANGE

FENERGO CLIENT LIFECYCLE MANAGEMENT is developed by and for banks to digitally transform how they manage customers and deliver exceptional customer experience – from initial compliance and onboarding, all the way through to regular and event-driven reviews.

visit us
www.fenergo.com

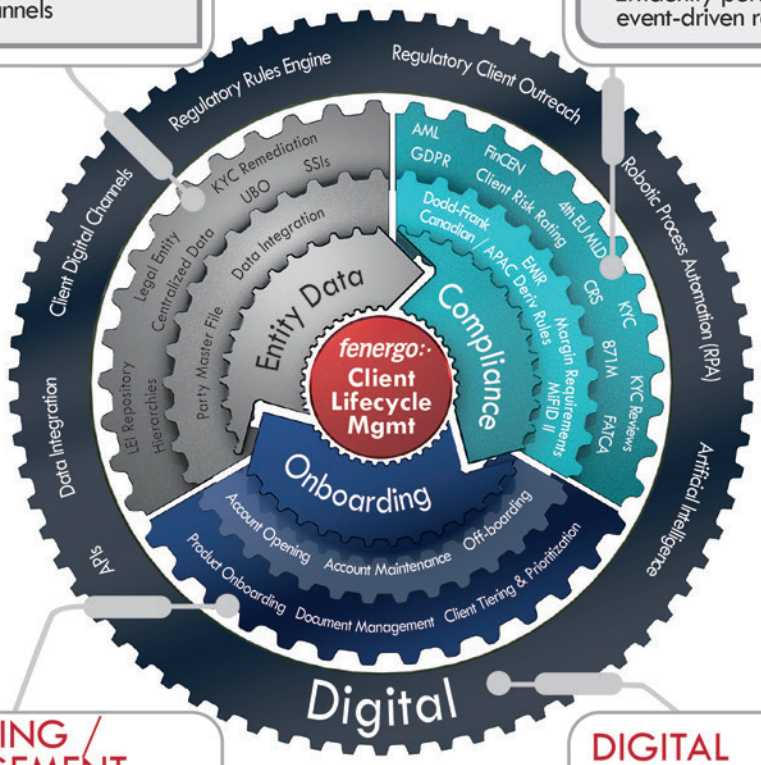
DATA MANAGEMENT

- Unlock 360-degree view of clients across business lines, functions & jurisdictions
- Re-use up to 75% of existing client data & documentation for new regulatory obligations
- Automate data & document collection through advanced digital channels

REGULATORY COMPLIANCE

- Comply with regulations across multiple regulatory frameworks
- Automate identification of in-scope regulations with Regulatory Rules Engine
- Efficiently perform regular KYC & event-driven reviews

THE INDUSTRY STANDARD



FOR CLIENT LIFECYCLE MANAGEMENT

CLIENT ONBOARDING / LIFECYCLE MANAGEMENT

- Improve efficiency and orchestration of client/ product onboarding across compliance, legal, credit, tech & ops
- Reduce client onboarding times by up to 80%
- Deliver an enhanced client experience

DIGITAL

- Perform regulatory client outreach through secure digital channels (Client Connect)
- Automatically consume data from multiple data providers through API integration tools
- Expedite compliance and KYC remediation with AI / RPA

FOR MORE INFORMATION ON FENERGO CLIENT LIFECYCLE MANAGEMENT:

www.fenergo.com info@fenergo.com

ACAMS®

NOMINATIONS ARE OPEN FOR THE

2018 ACAMS RECOGNITION AWARDS

ACAMS Recognition Awards are presented to members who have made outstanding contributions to our global community.

ACAMS TODAY
ARTICLE OF THE YEAR

ACAMS
AML Professional of the Year Award

SUBMIT YOUR NOMINATIONS

https://www.acamsconferences.org/vegas/awards/

SUBMISSION DEADLINE IS JULY 27