



ACAMS 
TODAY™



«RUSSIA'S HOPE OF»
ICE HOCKEY
Glory
BURIED UNDER
SANCTIONS

ALSO IN THIS ISSUE:

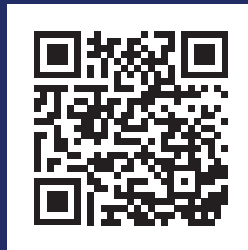
Trade finance
risk and controls



Build your network.
Expand your knowledge.
Elevate your career.

Attend an ACAMS event in 2023.

ACAMS events take place online and in-person across the globe. Scan the QR code to see our full calendar:



FinScan®

A complete KYC & AML solution

BUILT FOR RELIABILITY AND SCALE



Watchlist Screening



Transaction Screening



ID Validation



KYC & Risk Scoring



UBO Due Diligence

FinScan offers comprehensive KYC & AML regulatory checks from one user-friendly platform, with improved data quality for more accurate results. **Try it now and see the difference.**

Detecting AML risk in **180+** billion customer records across **65+** countries annually

verizon[✓]

AMOUNT

中国建设银行
China Construction Bank

IN
GO

Bupa بوبا

Amway

onyx
CLEARANCE

بنك الرياض
riyadh bank

Close Brothers

VOLVO
Financial Services

"We need a compliance tool that meets very high standards across a variety of areas. We've built a great partnership with FinScan that's helped lay a foundation for our continued growth and success."

Robbi Nagel, Deputy Global Chief Compliance Officer, AmTrust

www.finscan.com



DIRECTOR OF EDITORIAL CONTENT

Kieran Beer, CAMS

EDITOR-IN-CHIEF

Karla Monterrosa-Yancey, CAMS

The magazine for career-minded professionals in the anti-financial crime field

EDITORIAL AND DESIGN

SENIOR INTERNATIONAL EDITOR:
Monica Mendez, CAMS

EDITOR:
Benedict Bahner

ASSOCIATE EDITOR:
Ana Cecilia Martinez

CONTRIBUTING EDITOR:
Debbie Hitzeroth, CAMS-FCI

CREATIVE AND DESIGN:
Victoria Racine

EDITORIAL COMMITTEE

- Elaine Rudolph-Carter, CAMS
- Brian Arrington, CAMS
- Edwin (Ed) Beemer, CAMS-FCI
- Robert Goldfinger, CAMS
- Steve Gurdak, CAMS
- Jennifer Hanley-Giersch, CAMS-AUDIT
- Debbie Hitzeroth, CAMS-FCI
- Stacey Ivie, CAMS
- Anne Marie Lacourse
- Sanjeev Menon
- Ari Redbord
- Derek W. Smith, CAMS
- Joe Soniat, CAMS-FCI
- Amy Wotapka, CAMS

SENIOR LEADERSHIP TEAM

CEO:
Scott Liles

CHIEF PRODUCT OFFICER:
Angela Salter

CHIEF HUMAN RESOURCES OFFICER:
Bill Lumani

CHIEF SALES OFFICER:
David Karl

GLOBAL HEAD OF NEW VENTURES:
Hue Dang, CAMS-Audit

VP OF GLOBAL STRATEGIC COMMUNICATIONS & DEI:
Lash Kaur

CHIEF OPERATING OFFICER:
Mariah Gause

VP OF SANCTIONS, COMPLIANCE & RISK:
Justine Walker

ADVISORY BOARD

- CHAIR: Markus Schulz
- Sharon Campbell
- Jim Candelmo, CAMS
- Vasilios P. Chrisos, CAMS
- David Clark, CAMS, CGSS
- Howard Fields, CAMS
- William D. Langford, CAMS
- Dennis M. Lormel, CAMS
- Rick McDonell, CAMS
- Anthony L. Rodriguez, CAMS, CPA
- Rick A. Small, CAMS, (Emeritus)
- John Smith
- Dan Stipano
- Philippe Vollot

SALES AND REGIONAL REPRESENTATIVES

SENIOR DIRECTOR OF SALES AMERICA, CANADA AND LATIN AMERICA:
Sonia Leon, CAMS-Audit

DIRECTOR OF SALES GOVERNMENT/LAW ENFORCEMENT AND ADVISORY:
Jose Victor Lewis, CAMS

DIRECTOR OF SALES EUROPE:
Paolo Munari

DIRECTOR OF SALES MIDDLE EAST & AFRICA:
Michel Nassif

HEAD OF CARIBBEAN:
Denise Perez, CAMS

DIRECTOR OF SPONSORSHIP AND ADVERTISING DEVELOPMENT:
Andrea Winter, CAMS

HEAD OF SALES, APAC:
Christine Lim

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.

ACAMS Today © 2023 published by ACAMS. All rights reserved. Reproduction of any material from this issue, in whole or in part, without express written permission of ACAMS is strictly prohibited.



ACAMS — Global Headquarters 1100 Brickell Bay Drive #311090, Miami, FL 33131, USA
 Phone: 1-305-373-0020/1-866-256-8270 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



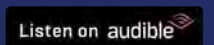
SANCTIONS SPACE

with Dr. Justine Walker



FINANCIAL CRIME MATTERS

with Kieran Beer





CONTENTS

ON THE COVER:

78 **Russia's hope of ice hockey glory buried under sanctions**

Discover how the Russian Kontinental Hockey League, seemingly destined for success, was put on ice following Russia's invasion of Ukraine.

ALSO ON THE COVER:

32 **Trade finance risk and controls**

An overview of trade finance, the risks it may present and the due diligence and controls necessary to keep financial crime in check.





10
From the editor

12
Member spotlights

14
From the director of editorial content

AML CHALLENGES

16
2023: Evolving threats and risk landscapes require investment in technology
A look at why regulated entities need to strengthen their defenses against financial crime risk and the steps they can take to do so.

20
The BSA tractor
Learn how the right training can help LE get the most out of using the BSA.

24
Why FIs should consider banking marijuana dispensaries

Uncovering the unexpected benefits associated with banking cannabis businesses.

26
The hawala system: A risky alternative to traditional banking

An overview of the concept of hawala and the risks associated with this value transfer system.

PRACTICAL SOLUTIONS

40
The great divide: Getting convergence right this time

A look at the convergence of AML, fraud and cybersecurity and the challenges and opportunities it presents for FIs and LE agencies.

46
The big impacts of small, in-house BMAs: A case study in the fight against corruption

How the adoption of in-house BMAs can produce meaningful results in AFC work and help businesses with their "future-readiness" in AML compliance.

54
The rise of real estate money laundering
Understand the lure of real estate transactions for money launderers, as well as the phases of real estate money laundering and common indicators of this type of crime.

62
Choppy waters: Negotiating the complexities of sanctions due diligence in an uncertain world

Find out why companies should regard sanctions due diligence as a necessity when considering cross-border transactions.



INTERVIEW

68

**Edwin W. Harris Jr.:
Eradicating corruption in West Africa**

ACAMS Today talked to Edwin W. Harris Jr. about his role in fighting money laundering in West Africa and what led him to be an AFC advocate.

COMPLIANCE

70

Defining ‘digital asset-related business’

Learn what digital asset-related businesses are and how they can be classified into three relevant risk-based tiers.

74

**Eyeing compliance blind spots
in bank-fintech partnerships**

A look at the growing trend of banks forging partnerships with fintechs and the compliance challenges these alliances may present.

GLOBAL FINANCIAL CRIME REVIEW

84

**Why terrorist organizations
use human trafficking**

Shedding light on the ways terrorists employ human trafficking to support their activities, including sexual exploitation, labor exploitation and driving recruitment efforts.

94

AML POLICY

90

FinCEN’s terrorist financing policies

A detailed view of terrorist financing, why it was named one of FinCEN’s national AML priorities and the red flags for detecting its occurrence.

94

Is it “Groundhog Day” for digital assets?

While 2022 represented a record-setting year for attacks on crypto businesses, 2023 is shaping up as a year for digital asset enforcement actions.

COMMUNITY BANKING CORNER

98

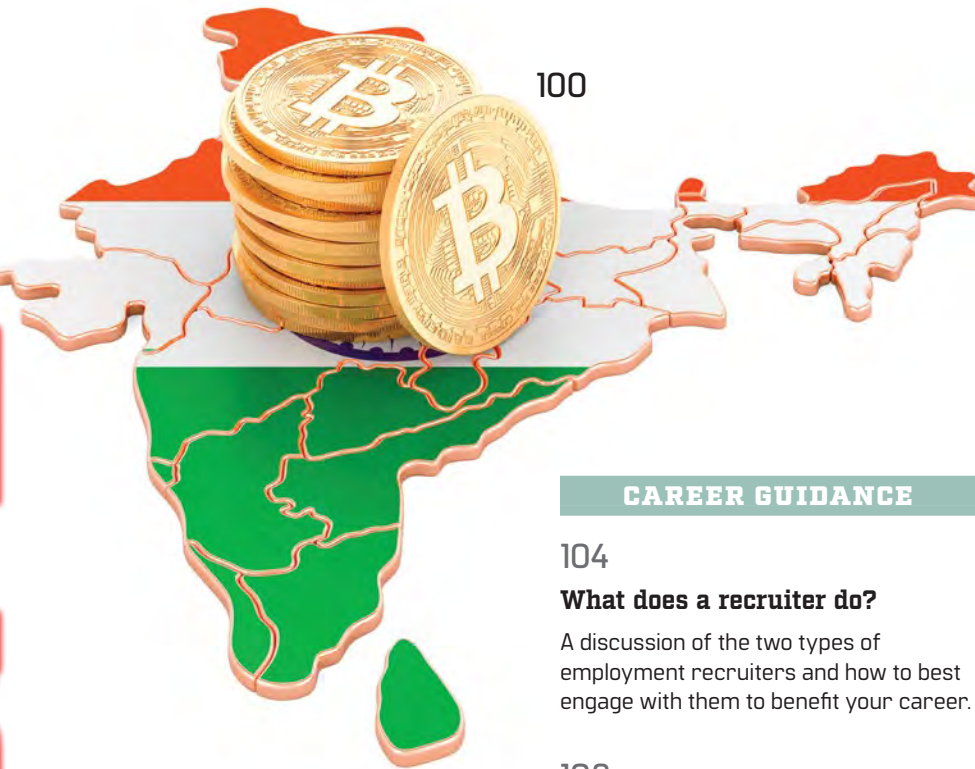
**Information sharing:
Why community banks should participate**

How clarification from FinCEN on Section 314 of the USA PATRIOT Act has cleared the path for community banks to participate in information sharing.



74





100

ASPECTS OF APAC

100

Regulatory ambiguity in India—Breeding ground for crypto criminals

Find out about the cryptocurrency regulation challenges facing India—the world’s largest cryptocurrency holder—and some of the infamous crypto scams that affected the country.

CAREER GUIDANCE

104

What does a recruiter do?

A discussion of the two types of employment recruiters and how to best engage with them to benefit your career.

108

Making the leap to management

Tips and strategies for AML professionals who are interested in steering their career to management.

MEET THE ACAMS STAFF

116

Lash Kaur: Bettering the world through social impact

KNOW YOUR CHAPTER

118

ACAMS South Florida Chapter

120

ACAMS Southern Nevada Chapter

124

ACAMS Italy Chapter

GRADUATES

128

Advanced graduates

130

CAMS graduates

138

CCAS graduates

140

CGSS graduates

SARSENSTRIPS™



Russia is in the penalty box



When you grow up in cold weather and in a place where the license plate tagline is “Greatest Snow on Earth” and where the 2002 Olympics were held, you tend to get involved in winter sports. My winter sport of choice was ice skating, but many of my friends were involved in ice hockey leagues. I spent a significant amount of time cheering them on as they competed at the rink. Part of the fun of watching hockey is the sheer physicality of the sport, where in some instances, depending on the foul committed, players are placed in a penalty box for an amount of time. Once the time is completed, they jump into the rink ready to play.

Like the players we see enter the penalty box for misconduct, Russia has also entered its own sanctions penalty box. The lead article, “Russia’s hope of ice hockey glory buried under sanctions,” details the demise of the Russian Kontinental Hockey League due to Russia’s invasion of Ukraine. The case study outlines what the results of sanctions on key Russian individuals have done to the once internationally renowned “Red Machine.”


Gliding along to the second headline article, “Trade finance risk and controls,” the authors give an overview of the risks of trade finance and how due diligence controls can help in keeping financial crime in check.

The anti-financial crime (AFC) industry is a team sport that requires a proper skill set; the article “The BSA tractor” outlines how proper training for law enforcement (LE) professionals can help them in maximizing the benefits of the Bank Secrecy Act.

There comes a point for every professional where they need to step up from the minor league to the major league. This edition includes tips and strategies to assist anti-money laundering (AML) professionals in taking the next step in their careers and joining management in the article titled “Making the leap to management.”

As in hockey, the key to success is a strong defense. In the article “Why terrorist organizations use human trafficking,” the author discusses how terrorist organizations profit from the use of human exploitation in the forms of sexual and labor trafficking. Without the human element and the continued abuse of such individuals, terrorist organizations would fall apart, especially if you also cut off their source of income. AML professionals can defend their institutions by learning these key concepts and how to implement a stronger strategy for dealing with human trafficking.

In a classic team-up situation, the article “The great divide: Getting convergence right this time” looks into the possible challenges and opportunities a union of AML, fraud and cyber could present for financial institutions and LE agencies.

I hope we can all keep our eye on the puck and strive to stop financial crime and steer the proverbial puck to “light the lamp” of efficient AFC compliance. 

Karla Monterrosa-Yancey

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

Crypto AML moves fast. Are you ready?

As crypto markets change, you need to be ready to react. CCAS - ACAMS' first crypto-focused AFC certification - will give you the skillset to navigate crypto financial crime risks.

Become one of our first certified crypto AFC specialists.

Visit www.acams.org/ccas

ACAMS 



Tarik Eker, CAMS—Germany

With over 25 years of experience in electrical engineering and computer science, and more than 15 years in the field of financial crime prevention, Tarik Eker, head of compliance and senior lecturer, is an expert in the fight against money laundering. Eker began his career as an electrical engineer in 1997 and quickly realized the potential for technology in the field of financial crime prevention. Since he transitioned to the financial industry, he has been at the forefront of detecting and preventing money laundering. In his current role as head of anti-money laundering (AML), he leads a team of experts in improving the company's AML program. Under his leadership, the company has been able to identify and investigate potential money laundering schemes more efficiently and effectively. One of the founding members of the ACAMS Germany Chapter, Eker is also a senior lecturer at the University Fresenius and ISM University of Management and Economics, where he lectures on forensics, compliance, ethics, governance, data science, quantitative analysis and operation research. He is dedicated not only to his work but also to the broader financial crime prevention community. Eker is a member of several industry groups and regularly participates in working groups and task forces to improve the fight against financial crime.



Derek W. Smith, MBA, CAMS, CRCMP—The Bahamas

Derek W. Smith, MBA, CAMS, CRCMP, is a senior contributor in the Bahamas' compliance and anti-money laundering (AML) space. He facilitates training in operational risk assessments, AML risk assessments, business continuity management, information security governance, organizational resilience and agility.

Currently, Smith serves as the assistant vice president of compliance and money laundering reporting officer (MLRO) for the CG Atlantic group family of companies (member of Coralisle Group Ltd.) in the Bahamas and Turks and Caicos. At CG, Smith's responsibilities include regulatory compliance for the group's Aruba, Curaçao, St. Lucia, and St. Vincent and the Grenadines. In addition, he is CG's compliance training lead throughout the Caribbean. Previously, Smith was the group compliance officer and MLRO at a TerraLex member law firm (Higgs & Johnson); the assistant vice president of Fiduciary Risk, assistant vice president of Compliance and assistant manager of Internal Audit at a Wolfsburg Group member bank (Citi); and an auditor and client accountant at Deloitte.

Smith is currently a board director of the ACAMS Bahamas Chapter and a past executive of the Bahamas Association of Compliance Officers (BACO). Moreover, he is a member of the *ACAMS Today* Editorial Committee.

He is a frequent business columnist on governance, risk, compliance, AML and information security topics, having written and published over 52 articles.

In Smith's nonprofit life, he is a member and past executive of Phi Beta Sigma Fraternity, Inc., and president of the Nassau Bahamas National Pan-Hellenic Council. In addition, he is the past rotary means business chair of Rotary District 7020 (a district covering 10 Caribbean countries). Currently, Smith is the membership area coordinator for the Rotary Clubs of the Bahamas.



Amy Wotapka, CAMS– Wisconsin, USA

Amy Wotapka, CAMS, is the Office of Foreign Assets Control and Bank Secrecy Act Officer at First American Bank. Wotapka's banking career started in 1982 as a teller, ultimately landing in anti-money laundering compliance in 2001 under her mentor Jackie Santos at PNC Bank. From there, Wotapka transitioned to Capital One in various management roles.

Over the past 20 years, Wotapka has enjoyed many volunteer positions with ACAMS. Wotapka is a founding member of the ACAMS Richmond Virginia Chapter. Wotapka was also privileged to be a member of the Chapter Steering Committee for ACAMS. In addition to her many years as an *ACAMS Today* Editorial Committee member, Wotapka has authored dozens of articles for *ACAMS Today*. She earned the ACAMS Article of the Year Award in 2010. She has also moderated and presented on multiple webinars for ACAMS and has presented at both the Hollywood and Las Vegas national conferences.

In addition to her extensive volunteer work with ACAMS, Wotapka has taught courses in Economics for Bankers and Macroeconomics at the American Institute of Banking. She has a passion for helping animals and has volunteered with multiple dog rescues.

Wotapka received a Bachelor of Science degree from Beaver College (now Arcadia University) in Pennsylvania. **AT**

QUIZ

Calling all *ACAMS Today* readers!

Assess your knowledge by taking the following quiz question from this issue:

According to the article “Russia’s hope of ice hockey glory buried under sanctions,” it was expected that Roman Rotenberg, son of Russian President Vladimir Putin’s childhood friend Boris Rotenberg, would be named head coach and CEO of the SKA Saint Petersburg ice hockey team as he has been professionally involved in the game for years.

- a. True
- b. False

DID YOU ANSWER CORRECTLY?

Visit the quiz index on
ACAMSToday.org for more
anti-financial crime quizzes!

(See bottom right of page for answer.)

Public interest versus privacy rights play out in CTA



In January 2021, the passage of the Anti-Money Laundering Act of 2020 (AMLA) was greeted with near jubilation by the anti-financial crime (AFC) community. Since then, regulations implementing the AMLA, specifically the Corporate Transparency Act (CTA) portion, have gotten a mixed reception from AFC professionals.

The act and the Financial Crime Enforcement Network's (FinCEN) enabling regulation will ultimately create a database of corporate ownership, beginning in January 2024. For the first time, federal law enforcement (LE), national security and intelligence agencies, and federal regulators will have direct access to beneficial ownership information in the context of "investigative and enforcement activities relating to civil or criminal violations of law," which covers a broad set of circumstances.¹

As with all legislation, however, compromises were made to pass the CTA between legislators who believed the public has a right to know who owns businesses operating in the U.S. and lawmakers who valued owners' privacy rights over the public interest.

The result is that the FinCEN regulations greatly limit who will have access to the ownership database.

Among those with limited access are state, local and tribal LE officials. They must send FinCEN a copy of a "court order" that authorizes them to seek information, along with a written explanation of why their query is relevant to their case.²

Financial institutions (FIs) will have to meet an even higher bar: They must obtain permission from clients to see a copy of their filing with FinCEN and they cannot share the ownership information they receive with foreign subsidiaries or

foreign domiciled back offices. Banks are only authorized to request the ownership information to fulfill their customer due diligence duties and not in relation to their reporting responsibilities under the Bank Secrecy Act. Money services businesses, including virtual asset service providers, have no standing to request filings.

Neither state and local LE nor banks can query the database, for example, to connect a corporate owner to multiple filings of the companies in which they may also hold an interest.

In commenting on these limitations, the American Bankers Association (ABA) was critical of FinCEN, concluding that under its notice of rulemaking the database is "practically useless." The February 14 missive to FinCEN, released on the last day of the open comment period and certainly no Valentine, called on FinCEN to scrap its "fatally flawed" proposal and start again.³

The public's legitimate interest in corporate ownership transparency has been fueled by numerous documented abuses of shell companies. The Panama Papers and Paradise Papers showed how political leaders hid wealth, some of it stolen, and transnational crooks made the proceeds of their crimes disappear through opaque shell companies.⁴ The uncovering of illicit fund flows from Russia through the Baltic States, into Nordic banks, and into the global financial system via shell companies also furthered the push for transparency.⁵

The abuse of shell companies continues, most notably to evade sanctions, a fascinating case study of which is *ACAMS Today's* cover story in this issue on page 78.

But the pushback on privacy grounds has been forceful.

European Union (EU) legislation for country-by-country ownership registries that would cascade into an EU-wide registry is being inconsistently implemented following an EU high court decision that full-public access violates privacy rights. The debate now centers on who should have access beyond "mere citizens," with the possibility remaining that FIs, nonprofits and journalists will have access, which means the EU registries are likely to remain more accessible than the U.S. registry.⁶

A case can be made for certain ownership information remaining private under limited circumstances, but others will have to make it. Quoted repeatedly, for good reason, is U.S. Supreme Court Justice Louis Brandeis' remark that "sunlight is the best disinfectant" for public corruption and crime.

It is an accomplishment that the U.S. will have a national registry of corporate ownership available to some of the LE community. But unfortunately, as currently configured, much of that information will not in the largest sense see the light of day. That will require further legislation and regulation. **AT**

Kieran Beer, CAMS
chief analyst, director of editorial content
Follow me on Twitter: @KieranBeer
"Financial Crime Matters with Kieran Beer"

¹ Benjamin Hardy, "Compliance Professionals, Former US Officials Debate FinCEN's 'Access' Proposal," *ACAMS moneylaundering.com*, February 9, 2023, <https://www.moneylaundering.com/news/compliance-professionals-former-us-officials-debate-fincens-access-proposal/>

² Ibid.

³ "American Bankers Association Rejects FinCEN's Latest Beneficial Ownership Plan," *ACAMS moneylaundering.com*, February 14, 2023, <https://www.moneylaundering.com/news/american-bankers-association-rejects-fincens-latest-beneficial-ownership-plan/>

⁴ "The Panama Papers: Exposing the Rogue Offshore Finance Industry," *The International Consortium of Investigative Journalists*, <https://www.icij.org/investigations/panama-papers/>

⁵ Benjamin Hardy, "Danske Bank Settles Money Laundering Accusations After Deceiving US Banks," *ACAMS moneylaundering.com*, December 13, 2022, <https://www.moneylaundering.com/news/danske-bank-settles-money-laundering-accusations-after-deceiving-us-banks/>

⁶ Koos Couvée, "Months After Landmark Ruling, EU's Ownership Databases Still Face Uncertain Future," *ACAMS moneylaundering.com*, February 13, 2023, <https://www.moneylaundering.com/news/months-after-landmark-ruling-eus-ownership-databases-still-face-uncertain-future/>

LOOKING FOR MORE ACAMS TODAY CONTENT?

Visit ACAMSToday.org!



ACAMS TODAY TM

In addition to our print publications, ACAMSToday.org features web-only content, including exclusive articles, interviews, interactive polls and more!

2023

The fight against money laundering is likely to get more challenging for many businesses in 2023, with global events likely shaping the compliance and regulatory landscape.

With organized criminals increasingly becoming more tech-savvy and regulators increasing enforcement action for noncompliance, the stakes have never been higher for regulated entities to strengthen their defenses against financial crime risks.

Increased regulatory enforcement

While the COVID-19 pandemic played a role in a lull in enforcement actions in 2021 and throughout 2022, we are likely to see increased regulatory enforcement for anti-money laundering (AML) compliance breaches in 2023, particularly given the continued financial crime risk management failings that have emerged around the globe during the last few years. Examples include the corrupt business practices and fraudulent financial reporting that led to the insolvency of Wirecard and Danske Bank, where these organizations pleaded guilty to defrauding U.S. banks in a multi-billion dollar scheme, resulting in a \$2 billion settlement.¹

We predict greater collaboration between law enforcement agencies, regulators and regulated entities to combat financial crime, such as the Fintel Alliance, which is pioneered by the Australian Transaction Reports and Analysis Centre (AUSTRAC) in Australia.² In addition to working closely with regulators, financial institutions are increasingly forming alliances through initiatives such as the Global Coalition to Fight Financial Crime, as they recognize the importance of working more collaboratively to share information and intelligence while establishing best practices to remain compliant.³

There is also likely to be a continued focus on internationally endorsed global standards against money laundering and terrorist financing. For example, in its last meeting, the Financial Action Task Force (FATF) published an action plan to combat terrorist financing, which highlighted the FATF countries' commitment to implementing significant changes to the international AML risk landscape resulting from the Russian invasion of Ukraine.

As a result, businesses may need to implement more stringent and effective AML/counter-terrorist financing (CTF) and sanction risk assessments and compliance programs to protect their international trade from organized criminal networks.

EVOLVING THREATS AND RISK LANDSCAPES REQUIRE INVESTMENT IN TECHNOLOGY

Greater personal accountability

In 2023, regulators worldwide will continue to focus on holding board members, senior executives, and responsible persons civilly or criminally liable for AML/CTF-related breaches. Expect to see an increased focus on how board decisions are made, including assessing the relationship between board members and in-house compliance and risk management teams.

This rise in the importance of personal accountability regimes will drive board members to pay closer attention and actively engage with their AML/CTF risk and compliance teams to gain a deeper understanding of the effectiveness of financial crime risk management controls. This focus will be crucial in successfully creating and embedding a strong compliance culture within organizations to help prevent financial crime and comply with regulatory standards.

With closer regulatory scrutiny, it is more important than ever for boards to clearly define their risk appetite for financial crime risks in the context of achieving their stated business objectives by defining the risk tolerance (or deviation from risk appetite) they are willing to accept. Boards must take an active role in ensuring their organization's design to implement and maintain a robust financial crime risk management framework that can identify and assess financial crime risks. In addition, boards should implement appropriate and proportionate controls to mitigate and manage identified risks based on their risk appetite.

Two possible frameworks include defining an AML/CTF risk methodology that is logical and defensible as well as defining the risk groups, risk categories, risk factors and risk indicators that are to be assessed.

Capability uplift

Traditional approaches to managing financial crime risks have led to massive compliance failures and material fines. AML/CTF laws are expanding to new sectors, meaning many newly regulated businesses may lack the basic understanding of managing financial crime risks. This is particularly true for small businesses that are struggling to keep up with regulations and lack the in-house capabilities to develop robust risk management and control frameworks.

Businesses that do not get this right the first time often need to implement AML/CTF program capability uplifts and expensive remediation projects to improve major elements of their AML/CTF compliance programs to meet their regulatory compliance obligations.

Enterprise-wide (or business-wide) risk assessments

There is a growing realization that spreadsheets are no longer sufficient to manage the increasingly complex and fundamentally important requirement of enterprise/business-wide risk assessments, which have many limitations compared with technology-enabled approaches.

We expect to see more businesses increase their investment in enterprise-wide financial crime risk assessment solutions to strengthen their approach in identifying, assessing, mitigating and managing financial crime risk exposures. A typical technology-enabled approach involves setting up a risk assessment framework, conducting simplified risk assessments across the organizations using technology, and documenting and tracking risk decisions using an audited workflow.

The emergence of specialized technologies to execute complex enterprise-wide risk assessments and the recognition that spreadsheets have many limitations in managing these processes effectively is making businesses evaluate the robustness of their processes. Many are looking at technology-enabled, human-led approaches using platforms because there is a growing realization that technology solutions offer benefits over traditional spreadsheet approaches. These include an audit trail, decision-driven workflows and aggregated real-time financial crime risk reporting, to name a few.

Organizations are considering different technology options in their budgets, depending on the nature, size and complexity of regulated businesses, and the level of maturity of their existing enterprise-wide money laundering risk assessment processes. Some companies choose to adopt guided solutions, where the methodology is pre-built into the platforms and which are suitable primarily for small and medium-sized

businesses. Larger, more complex and more sophisticated organizations that want to tailor their own risk methodology and build their own risk models with weightings and control libraries are looking to adopt highly configurable platforms, where they can control the inputs and outputs of the business-wide risk assessment from end-to-end.

Greater investment in technology

Many businesses will look to technology as an enabler for driving better financial crime risk management outcomes. This means there will likely be a significant increase in investment in regulatory technology (regtech) solutions in 2023 and beyond. Verified Market Research identified that in 2020, the global regtech market was worth approximately \$15 billion. By 2028, it is projected to reach \$87.17 billion.⁴

While many companies have attempted to build in-house enterprise-wide risk assessment solutions to remain compliant, using a best-in-class solution designed to assess financial crime risk will be essential in managing risks in a timely manner and delivering cost savings through significant process efficiencies.

With increased regulatory enforcement action and a constantly evolving threat and risk landscape by innovative criminal networks, businesses need to rise to the challenge by investing in technology and people with the skills and knowledge to improve their capabilities and capacities to fight financial crime.

In 2023, it will be more critical than ever for companies to maintain an effective financial crime risk and compliance control framework to reduce the risks of being exploited by organized criminal networks. Seeking expert guidance and using proven systems can help businesses remain compliant and protect themselves and their customers. AT

*Anthony Quinn, founder/CEO, Arctic Intelligence,
anthony.quinn@arctic-intelligence.com*

*Mark Smitherman, sales director, EMEA and North America,
Arctic Intelligence, mark.smitherman@arctic-intelligence.com*

¹ "Danske Bank Pleads Guilty to Fraud on U.S. Banks in Multi-Billion Dollar Scheme to Access the U.S. Financial System," *United States Department of Justice*, December 13, 2022, <https://www.justice.gov/opa/pr/danske-bank-pleads-guilty-fraud-us-banks-multi-billion-dollar-scheme-access-us-financial>

² "Fintel Alliance," *Australian Transaction Reports and Analysis Centre*, <https://www.austrac.gov.au/about-us/fintel-alliance>

³ Global Coalition to Fight Financial Crime, <https://www.gcffc.org/>

⁴ "RegTech Market Size Worth \$87.17 Billion, Globally, by 2028 at 23.92% CAGR: Verified Market Research®," *Cision PR Newswire*, March 8, 2022, <https://www.prnewswire.com/news-releases/regtech-market-size-worth--87-17-billion-globally-by-2028-at-23-92-cagr-verified-market-research-301497770.html>



Compliance. The Smart Way.

Multi-Award winning financial crime risk assessments to protect your business.



Our enterprise-wide financial crime risk assessment platforms are trusted by hundreds of regulated businesses in over 20 industries and 15 countries.

AML ACCELERATE

Enterprise-wide money laundering and terrorism financing risk assessment and AML policy platform designed for small and medium sized businesses.

RISK ASSESSMENT

Fully configurable financial crime risk assessment platform designed for larger enterprises that want to tailor their own risk and control models.

Book a demo today

✉ info@arctic-intelligence.com

🌐 arctic-intelligence.com


Risk modules available for:

- Money Laundering
- Terrorism Financing
- Sanctions
- Bribery and Corruption
- Fraud
- Correspondent Banking
- Modern Day Slavery
- Wildlife Trafficking

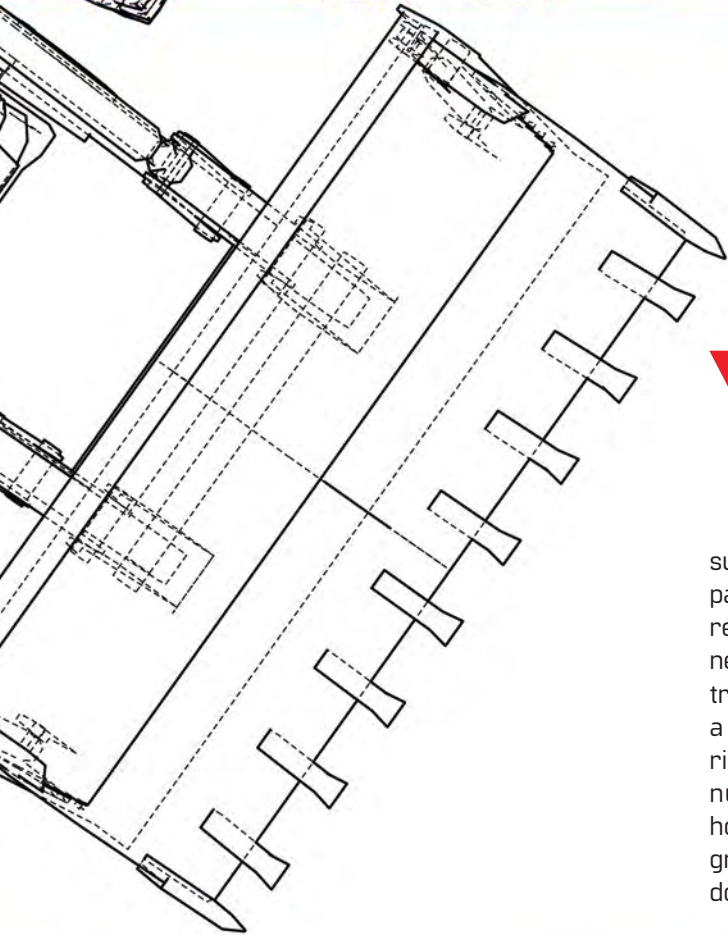
☎ Australia+61 (0) 2 8001 6433
Hong Kong +852 (0) 8197 4022
New Zealand +64 (0) 9889 3324

Singapore +65 6817 8650
United Kingdom +44 20 8157 0122

USA +1 646 475 3718
Canada +1 613 5188002

A detailed technical line drawing of a tractor, shown from a side-rear perspective. The drawing is rendered in black lines on a white background, with some parts highlighted in yellow. The tractor's components, including the engine, transmission, and rear axle, are clearly visible. The drawing is set against a background of yellow and black patterns, including a dotted pattern at the top and a striped pattern at the bottom.

THE BSA TRACTOR



You may have read it in magazines or seen the news or videos of some altruistic country sending modern tractors to aid farmers in developing nations. It seems surprising when they return later to find all the tractors in disrepair, with some now even being pulled by teams of horses. Some reactions blame the farmers for either ignorance or ungratefulness. The fact is that this was an unrecognized and unaddressed training issue. These farmers instinctively know that tractors are a better option for more efficient farming tasks, yet their experiences are within a culture that is unfamiliar with all the other nuances required to use and maintain tractors. They had, however, learned the many nuances of how to feed, house and groom the horses that did the task prior. Not knowing what we do not know is a classic training challenge.



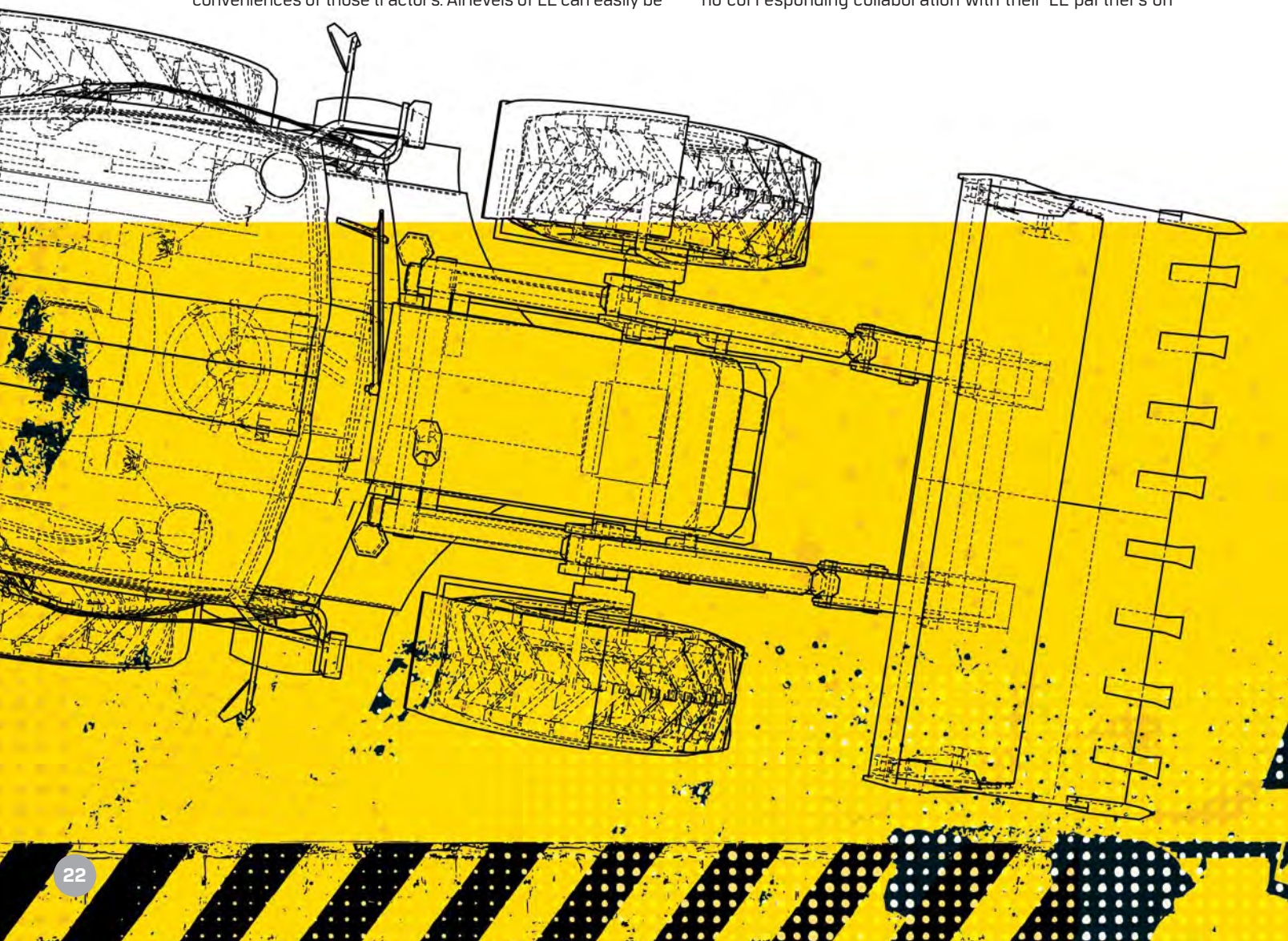
Law enforcement (LE) and the Bank Secrecy Act (BSA)

For far too many in LE, a similar analogy can be made with the BSA, which has been similarly gifted to them for their investigations. Most LE investigators instinctively know that a "follow-the-money" investigative strategy is sensible and offers a viable investigative option, yet their experiences are in an investigative culture where this kind of financial intelligence and information was not readily available or easy to obtain. The investigative models they developed worked around that. Along came the BSA, like the tractors, offering some superior investigative options, yet it was delivered with the same assumptions as those tractors. Many crucial nuances of what a follow-the-money investigative strategy entailed were not part of the existing LE culture. Investigators, just like the farmers, adapted bits and pieces of BSA offerings, yet they too often reverted to what they knew outside of those limited applications.

Ignorance or ungratefulness is not part of this equation. With just a little more basic training, most of those farmers will quickly appreciate and adapt to the usefulness and conveniences of those tractors. All levels of LE can easily be

trained in basic financial investigation literacy, but providing that basic training is essential. The nuances of a follow-the-money investigative strategy are not difficult to comprehend but need to be a larger part of the training model. To accept the virtues of the tractors, those farmers also have to accept and rely on new partnerships as well as delegate responsibilities to other specialists with whom they were unfamiliar. There is a big difference between shoeing a horse and changing a tire. LE, like the farmers, traditionally exudes a culture of self-reliance. These new partnerships outside of those cultures are not always immediately or easily accepted.

The prevailing investigative strategies and cultures are often more difficult to overcome than any lack of abilities. Those in the private sector anti-money laundering (AML)/BSA compliance community have made great strides in identifying suspicious financial behaviors, intelligence and even evidence of criminal underpinnings. They virtually created many nuances we now refer to as suspicious activities. While those in the AML/BSA compliance community regularly isolated and identified these behaviors, there was no corresponding collaboration with their LE partners on



incorporating them into comprehensive criminal investigation schemes. They kept improving the tractor despite many prevailing and unresolved issues in the basic operations.

The primary federal LE agencies have done an excellent job in using the BSA to identify, seize and/or forfeit ill-gotten gains. Recovering money for victims of fraud, taking money from narcotics traffickers and stopping the funding of terrorists alone makes the BSA valuable. Beyond that, there are many more valuable unexplored and underused virtues of the BSA. These essential nuances of this BSA tractor need to be better known to a far broader sector of LE efforts and their investigative strategies. Following the money is too often perceived as a math issue when it is a training and evidentiary one. The amounts are secondary to the transactional activity identified, the same way finding contraband is essential before how much contraband has any relevance.

Facilitating crime through common lies and oversight

It is nearly impossible to participate in criminal activity without creating corresponding identifiable indicators within your financial activities. Our money has evolved into our primary societal survival tool. Being so, it also is the primary motivator behind the crime. It was that realization that led to the government providing the versatile BSA. With proper analysis and interpretation, our income, spending and handling of finances can define us better than our social media profile. Imagine the investigative potential of combining both of those.

In legal and social settings, it is common to lie about our finances. Financial truths can sometimes be unflattering or downright embarrassing if fully known by our family, friends and other associates. The reality is our bankers often know us better than our doctors. Criminals commonly take advantage of this propensity to lie about money. They also take advantage of how rarely those lies are ever challenged.

We generally avoid conversations that pry too much into personal finance issues. Those vulnerabilities are greatly amplified when criminal activity is involved. In financial investigations, there are no acceptable lies. What the money says will often be substantially different from what the people speaking for it say.


How often have you seen or read news stories of arrested scoundrels that include details of all the opulent spending and purchases they made before they were caught? Sports cars, jewelry and designer clothes are as common for criminals as for big lottery winners. The financial clues were there long before these culprits were apprehended. The BSA likely already had identified these clues and suspicions ahead of this unusual spending. With too few primary investigative strategies offering a financial-first approach, these clues and suspicions too often go unheeded and unaddressed. These cases seem to garner investigative attention only when other aspects and evidence of the crimes that produced them are exposed. The BSA recognizes that questioning the money should not be in hindsight or a secondary consideration.

Money motivates almost everything we do and virtually everything when it comes to crime. Although it should have naturally become a primary guiding principle in more investigation strategies, it was a mistake to assume that acceptance would not require substantially more basic training. The prevailing and existing investigative models and schemes are deeply embedded throughout the entire criminal justice system. While following the money makes sense, investigators, prosecutors, judges and even juries are much more used to seeing the more visual manifestations of crimes committed in the illicit quests for that money. The drug dealer with piles of powders, pills, weapons and currency does paint a good picture for prosecutors to present to a jury. Making the case that the money trail is often more important to the criminal justice mission will be an essential part of this BSA learning curve.

Conclusion

In the end, criminals want and need all the same life necessities and excesses that legitimate people do. Once you learn to follow the money, you start to identify and recognize that those two financial paths have identifiable differences. Things like currency, taxes and traditional paper trails in legitimate life present obstacles to covering up illicit incomes. This often manifests itself the most in some of the more mundane aspects of finances. When you take a closer look at most big cases in the news, you will often find deeper in the story that the big break was a little mistake involving one of these otherwise mundane items.

With suspicions starting with identifiable variances from normal, it is important to establish what normal is. Learning precisely how routine life expenses are paid is a prerequisite in starting down the illicit money trail. Separating a paycheck-to-paycheck life from a crime-to-crime life is not that difficult when investigators make the same efforts with the financials as they make when considering the other evidence and leads they commonly look for.

Courtesy of Sherlock Holmes, magnifying glasses and trench coats have become the universal symbols of detective work. The BSA simply offers investigators a new lens to look through. When you focus on the activities, you will start to appreciate that the math becoming out of focus is the whole point. The larger movements of money come into more illicit focus when taking a closer look at those little details. The BSA is a beautiful tractor; though, more of LE needs to take a closer look at the owner's manual. 

Steve Gurdak, CAMS, manager, Washington Baltimore HIDTA, Northern Virginia Financial Initiative (NVFI), 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.

WHY FIS SHOULD CONSIDER

BANKING

marijuana

DISPENSARIES

Former Financial Crime Enforcement Network (FinCEN) Director Kenneth Blanco once said, "Banks must be thinking about their crypto exposure. If banks are not thinking about these issues, it will be apparent when examiners visit."¹ This advice from the former FinCEN director can also be applied to marijuana banking; financial institutions (FIs) cannot ignore the marijuana industry and expect not to be exposed to the risk associated with the industry. In addition, if FIs ignore the marijuana industry, they will also be losing out on future customers as well as potentially losing current customers, which translates to the FI missing out on a new revenue source. Global cannabis sales are expected to increase from \$13.4 billion in 2020 to \$148.9 billion by 2031.² With these projected figures, FIs cannot ignore the risk and opportunities the marijuana industry has to offer. By embracing a marijuana banking program, FIs can better manage anti-money laundering (AML) and regulatory risk, as well as establish a new revenue stream with new and existing customers.

From a risk-based perspective

FIs need to be aware of current and future activity in the marijuana industry to properly develop policies and procedures regarding marijuana banking. Many FIs that ignore marijuana dispensaries or create policies stating they will not bank marijuana dispensaries may be unintentionally limiting their level of AML risk monitoring with current customers, which is required by FinCEN.³ An FI with a properly developed marijuana program will have the tools to detect marijuana activity that an FI with a nonspecialized monitoring system would have otherwise missed. For example, has your existing customer with a convenience store started selling marijuana products? Has your loan customer who rents commercial real estate started renting to a marijuana dispensary, and now your loan payments are derived from marijuana sales? Without a properly developed marijuana program, situations like the examples mentioned will be more difficult to detect. FIs that embrace a marijuana banking program will not only have the tools to detect unexpected marijuana activity but will also have the banking products needed to continue a banking relationship with their customers as opposed to having to exit the banking relationship due to a policy that states the FI will not bank a marijuana dispensary.

From an AML perspective

By banking marijuana dispensaries, FIs can help reduce the amount of financial crime in the industry. People start businesses, regardless of the industry, to make money and that money is usually deposited and used through the banking system. By refusing to bank marijuana dispensaries that are legally licensed by the state, FIs may be inadvertently driving owners of marijuana dispensaries to resort to money laundering and other financial crime tactics to get the income generated by their business, which is legal under state law, into the banking system. This will result in an increase in the number of suspicious activity reports (SARs) issued by FIs, which also means FIs will have to increase monitoring measures per FinCEN guidance,⁴ and possibly staffing to cope with the

increased activity from refusing to bank marijuana dispensaries. While filing marijuana SARs and the continuation SARs may seem tedious, filing SARs on an existing customer who turns out to have marijuana dispensaries and started committing financial crimes will be costly when the FI must exit the relationship. This will also bring more scrutiny from examiners and increase the liability of fines. FIs that do adopt marijuana programs and bank marijuana dispensaries will be able to offset the cost of increased monitoring from the income generated by the banking fees from marijuana dispensary customers.

There is also a financial benefit for FIs to bank marijuana dispensaries. As mentioned throughout this article, FIs that choose to bank marijuana dispensaries will not only be able to keep existing customers who choose to start marijuana dispensaries but also bank new and upcoming marijuana dispensaries. Choosing to bank marijuana dispensaries early will allow FIs access to a customer base with little competition. FIs that bank marijuana dispensaries will also be able to charge fees for servicing and monitoring marijuana dispensary accounts, increasing the FI's total profit generated from fee income. As more states legalize marijuana and more FIs begin to accept the banking of marijuana dispensaries, there will only be a brief period for FIs to take advantage of a potentially lucrative market with few competitors.

Conclusion

While marijuana has traditionally been avoided by the banking industry due to its illegal classification, the changes in state laws and evolving economic markets present new opportunities for FIs. Just as cryptocurrency started as a novelty and has become a new industry in the financial and compliance fields, marijuana and marijuana dispensaries are also gaining momentum with no signs of slowing down. As time goes on, more states will pass laws legalizing marijuana and FinCEN has and continues to provide guidance to FIs that choose to bank marijuana dispensaries. As the marijuana industry continues to grow, FIs are able to take advantage of the opportunity to increase their revenue streams and bolster their risk-monitoring processes as well. AT

Julius Bosco, CAMS, BSA specialist, The Citizens Bank of Philadelphia, Mississippi, MS, jsbosco3@gmail.com, LinkedIn

¹ Russell Sommers, "Cryptocurrency: The Risk Banks Already Have," *BankDirector.com*, October 8, 2021, <https://www.bankdirector.com/committees/risk-committees/cryptocurrency-the-risk-banks-already-have/>

² "Global Cannabis Market to Reach \$148.9 Billion by 2031," *Allied Market Research*, <https://www.alliedmarketresearch.com/press-release/cannabis-market.html>

³ "BSA Expectations Regarding Marijuana-Related Businesses," *Financial Crime Enforcement Network*, February 14, 2014, <https://www.fincen.gov/resources/statutes-regulations/guidance/bsa-expectations-regarding-marijuana-related-businesses>

⁴ *Ibid.*





THE HAWALA SYSTEM:

A RISKY ALTERNATIVE TO TRADITIONAL BANKING

Hawala, also known as hundi, is a traditional informal value transfer system that is not regulated in many countries. It relies on a network of hawala brokers (hawaladars), who transfer money on behalf of clients without the use of a traditional financial institution (FI). It is believed to have originated in ancient India and was later adopted in the Middle East and other regions, including the Horn of Africa and South Asia.

The hawala system is based on trust and relies on hawaladars who facilitate the transfer of funds from one person to another. Hawaladars in different locations are connected to each other through a network of relationships, and they use various methods to transfer funds, such as courier services or the internet. Hawala has traditionally been used as a way to transfer money internationally, especially in countries where there are restrictions on the movement of money or where the formal banking system is not well developed. It has also been used by migrant workers to send funds to their families in their home countries.

While it largely remains outside the formal financial sector and is therefore not subject to the same regulatory oversight as traditional FIs, some countries have taken steps to formalize and regulate the hawala system in order to address concerns about money laundering and other illicit activities. For example, in the United Arab Emirates (UAE) and the U.K., hawala is regulated by the Central Bank of the UAE and the HM Revenue and Customs (HMRC), respectively. The Central Bank of the UAE and the HMRC have implemented rules requiring that hawaladars register with them and follow certain reporting and record-keeping requirements.

HAWALA HAS BEEN USED BY SOME INDIVIDUALS AND ORGANIZATIONS TO BYPASS FINANCIAL SANCTIONS OR TO EVADE DETECTION BY AUTHORITIES

In other countries, hawala remains largely unregulated, which can make it vulnerable to abuse. It is important to note that using hawala carries certain risks, including the potential for fraud or loss of funds. There also may be limited recourse if something goes wrong.

How the hawala system works

Below is how the hawala system typically works:

1. A client or sender approaches a hawaladar and asks to transfer money to a recipient, or beneficiary, in another location.
2. The hawaladar and the sender agree on a password or code that will be used to identify the transaction.
3. The sender gives the hawaladar the amount of money to be transferred plus a fee for the service. The fee is typically based on a percentage of the amount being transferred.
4. The hawaladar contacts a colleague or counterpart in the recipient's location and provides the details of the transaction, including the password or code.
5. The counterpart in the recipient's location receives the password or code and gives the recipient the agreed-upon amount of money.
6. The hawaladars settle their accounts at a later date, either through the transfer of funds or by balancing their accounts with other transactions.

Why hawala?

Some reasons why people might use hawala include:

- **Speed:** Hawala transactions can often be completed quickly, making it a convenient option for people who need to transfer money on short notice.
- **Low cost:** Hawala fees are typically lower than those charged by traditional FIs, making it an affordable option for people who need to transfer small amounts of money.

- **Discretion:** Because hawala transactions are not documented, they offer a level of privacy that is not available with traditional FIs. This can appeal to people who want to keep their financial affairs private.
- **Ease of use:** Hawaladars are often located in convenient locations, such as markets or small shops, making it easy for people to access their services.

How hawala providers make money

In addition to fees, hawaladars regularly make their profits by bypassing official exchange rates. Commonly, the payment enters the system in the sender country's currency and leaves the system in the pay-out country's currency.

Risks associated with using unregulated hawala

There are several risks associated with using unregulated hawala, including:

1. **Fraud:** Because hawala transactions are based on trust and personal connections, and there is no formal documentation or record keeping involved, there is a risk of fraud. Hawaladars may not be held accountable if they fail to deliver the funds as promised or if they use the money for their own purposes.
2. **Loss of funds:** There is a risk of losing funds when using hawala, either due to fraud or due to mistakes or errors in the transfer process. Because there is no formal dispute resolution process, it may be difficult to recover lost funds.
3. **Illicit activities:** Unregulated hawala can be used to facilitate money laundering, terrorist financing and other illicit activities. This can expose individuals who use hawala to legal and financial risks.
4. **Volatility:** The value of the funds being transferred through hawala may be affected by fluctuations in exchange rates or other market conditions. This can result in the recipient receiving less than the agreed-upon amount.

Hawala has been used by some individuals and organizations to bypass financial sanctions or to evade detection by authorities. For example, hawala has been used to transfer funds to countries or groups subject to international sanctions, such as Iran or Hamas. Because hawala transactions are not documented and rely on personal connections, they can be difficult to trace and can be used to evade detection.

There have been several cases in which hawala has been implicated in financial scandals or used to facilitate illegal activities. Here is an example of a real case involving hawala:



In 2015, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced that it had imposed sanctions on a network of individuals and companies based in Afghanistan and Pakistan for using the hawala system to facilitate the sale of opium and other illicit drugs. The individuals and companies were accused of using the hawala system to transfer funds to the Taliban and other terrorist organizations, as well as to launder the proceeds of drug trafficking. OFAC designated the individuals and companies as "Specially Designated Narcotics Traffickers" and imposed financial sanctions on them, including freezing their assets and prohibiting transactions with them.¹

This case illustrates the potential for hawala to be used to facilitate illegal activities, such as drug trafficking, and the risks that individuals and organizations may face if they use hawala to engage in such activities. It is important to note that using hawala to facilitate illegal activities is illegal in many countries, and individuals and organizations that are found to be doing so may face criminal charges and financial penalties.

Why hawala should be regulated

There are several reasons why some people believe that hawala should be regulated:

- **To reduce the risk of fraud and loss of funds:** Regulating hawala could help reduce these risks by establishing minimum standards and providing a formal dispute resolution process.
- **To prevent illicit activities:** Regulation could help prevent these activities by requiring hawaladars to comply with anti-money laundering and counter-terrorist financing rules and providing authorities with the tools to trace and investigate suspicious transactions.
- **To improve financial inclusion:** Regulation could help bring these people into the formal financial sector, providing them with access to a wider range of financial services and protections.
- **To promote financial stability:** Regulating hawala could help improve the overall stability of the financial system by reducing the risk of money laundering, terrorist financing and other illicit activities that can undermine the stability of the financial system.

How hawala may impact the banking system

Hawala can affect the banking system in several ways:

1. **Competition:** Hawala can compete with traditional FIs for a share of the money transfer market. In some cases, hawala may be able to offer lower fees or faster service, which could lead people to choose hawala over traditional FIs.
2. **Illicit activities:** If hawala is used to facilitate illicit activities, it could undermine the stability and integrity of the financial system.
3. **Financial inclusion:** If hawala can bring people into the formal financial sector, it could positively impact financial inclusion.
4. **Regulation:** Depending on the specific context, the use of hawala may require regulatory intervention to address concerns about money laundering, terrorist financing and other illicit activities. This could create additional costs and burdens for hawaladars and their clients and may also impact the banking system in other ways.

Overall, the impact of hawala on the banking system will depend on a variety of factors, including the extent to which hawala is used, the specific regulatory environment and the goals that are being pursued. In some cases, hawala may pose a competitive threat to traditional FIs, while in other cases, it may offer an opportunity to expand access to financial services and promote financial inclusion. It is important to carefully consider the potential impacts of hawala on the banking system in order to determine the appropriate balance between regulation and innovation.

Why regulating hawala seems to be challenging

There are several reasons why it is difficult to regulate hawala:

1. **Hawala operates outside of the formal financial system:** Because hawala is informal and operates outside of the formal banking system, it is more difficult for governments to monitor and regulate. In addition, hawaladars do not typically keep formal records of transactions, making it difficult to track the movement of funds.
2. **Hawala is based on trust:** The hawala system relies on trust between hawaladars and their clients. This makes it difficult for regulators to ensure compliance with laws and regulations.

3. **Hawala is a global network:** Hawala operates on a global scale, with hawaladars in different countries connected through a network of relationships. This makes it difficult for a single government to regulate the system effectively.

4. **Hawala has legitimate uses:** While Hawala has the potential to be used for illicit purposes, it is also used for legitimate purposes, such as transferring money internationally in countries with underdeveloped formal banking systems. This makes it difficult to regulate the system without affecting legitimate users.

Overall, the complexity and informality of the hawala system make it difficult for governments to effectively regulate and monitor its activities.

Conclusion

Hawala is an informal transfer system that has been used for centuries in many parts of the world. It is based on trust and relies on a network of hawaladars, who facilitate the transfer of funds from one person to another. While hawala has traditionally been used to transfer money internationally, especially in countries where the formal banking system is not well developed, it has also gained attention due to its potential role in money laundering and terrorist financing. The use of hawala in the context of money laundering and terrorist financing presents a significant challenge to governments and law enforcement agencies, as it can be difficult to detect and disrupt these activities.

Some governments have taken steps to regulate the hawala system, but it remains largely informal and operates outside of the formal financial system. Overall, hawala is a complex and multifaceted system with both benefits and risks, and it continues to play a significant role in the global economy. **AT**

Mohamed Abouzied, CAMS, CFE, CGSS, compliance advisory manager—Middle East and Africa, mdyazan@gmail.com

¹ "Financial flows linked to the production and trafficking of Afghan opiates," *Financial Action Task Force*, June 2014, <https://www.fatf-gafi.org/en/publications/MethodsandTrends/Financial-flows-afghan-opiates.html>



Trade finance risk and controls

Trade finance is described as the provision of finance and services by financial institutions (FIs) for the movement of goods and services between two points, either within a country or across borders.¹ There are multiple methods by which an FI can participate in the financing of product movement. The type of trade finance transaction and the role the FI plays in the transaction is the starting point for determining the risk of the transaction to the FI. In a risk-based anti-financial crime (AFC) program, determining the risk is critical as the risk level drives the amount of due diligence to be performed and the controls enacted.

There are multiple types of trade finance transactions.² There are multiple parties³ in a trade finance transaction. There are multiple risks associated with each letter of the credit transaction. For example, fraud risk is associated with forged/fraudulent documents or the submission of documents to multiple institutions for financing of the same product (multiple financing). This article, however, focuses solely on the money laundering (and related) risks to a bank issuing a letter of credit (issuing bank).

Generally, money laundering through loan products represents a lower risk than activity through transactional-type products (e.g., demand deposit accounts). Trade finance lending is an exception to that rule. Trade finance lending is an entrenched avenue for trade-based money laundering (TBML) and is thus at higher risk for money laundering than traditional lending products. The Financial Action Task Force defines TBML as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin.⁴ Money laundering through trade finance transactions can occur at any point during the money laundering cycle—placement, layering or integration.





Trade finance risks

The following risks may be present when an issuing bank participates in a trade finance transaction. The list below is not exhaustive and not every risk listed will be present with every trade finance transaction.

- The nexus in international trade.
 - Due diligence may be more difficult, especially for smaller issuing banks that may not have the resources to conduct international due diligence.
 - International trade transactions are complex. The supply chains between nations that source raw materials, the manufacturing countries that make and process them, and then the consumer nations that put the final products to use are all underpinned by similarly complex trade financing, making it possible.⁵ Involvement of higher risk or embargoed and sanctioned countries, where a shipment can lawfully go, with the destination country as the primary determinant, involves the consideration of both internal and external factors. Trade embargoes, sanctions and national licensing policies govern which goods, services and currency may be exchanged, to which countries, as well as if an export license or import permit will be required prior to outbound shipment. These external rules are legally binding policy mechanisms with strict operational expectations, accompanied by harsh penalties for violations. An FI's involvement in countries that may not be sanctioned or embargoed but have internal factors indicating a higher level of compliance risk will require robust due diligence and, oftentimes, commercial discussions to minimize risk exposure.
 - Capital flight occurs when there are large outflows of capital (assets or money) from a country, usually due to a negative macroeconomic environment such as political upheaval or high inflation. Evaders can avoid capital flight restrictions using trade by (1) utilizing over- and under-invoicing to get funds out of the country or (2) creating fake trades.
 - The trade finance transaction may be the only relationship the customer has with the issuing bank—the lack of transactional history heightens risk. In addition, indirect exports—selling products to often unknown customers in another country via an intermediary company—are increasingly routine within international trade and can bring substantially more risk to an FI.
 - The ease with which documents and websites can be forged or altered—using editing software, artificial intelligence and Chat Generative Pre-Trained



Transformer⁶ (ChatGPT) technology—offer easier and faster methods to create documents than in the old days of using white-out or cut and paste.

- Export control risk needs continual monitoring as regulations address trade. Controls are evolving, increasing in scope and generally becoming more nuanced.
- Ports may be out of footprint, so visual inspections of the product may be difficult or impossible and transshipment trade—shipment of goods via one or more intermediate locations or modes of transportation—make commodity verification and valuation more challenging.
- There is a multitude of traditional money laundering schemes.
 - ▲ Over- or under-invoicing to launder funds
 - ▲ Black market peso exchange⁷
 - ▲ Multiple invoices for the same products—occurs when the exporter invoices multiple times for the same shipment, transferring greater value from the importer to the exporter. Reassuringly, information systems are getting better at spotting these types of anomalies to proactively alert compliance staff to under- or over-invoice/multi-use shipment documents and similar schemes
- Export licensing involves risks.



At a minimum, an issuing bank must conduct enough due diligence on the applicant, beneficiary and all FIs involved in order to make a reasonable risk assessment of the transaction

- ▲ Not obtaining licenses
- ▲ Receiving fraudulent licenses
- ▲ Unknowingly transacting in dual-use goods requiring a license
- ▲ Country-specific product risk
- Transacting with denied parties
- Anti-boycott violations risk
- There is a risk of economic sanctions.
 - Financing products that violate an economic sanction
 - Transacting with sanctioned parties, including but not limited to sanctioned vessels
- Inconsistencies can occur.
 - Product, the dollar value of the transaction, counterparties or route is inconsistent with an existing customer's usual transactional pattern
 - Unusual or unexpected payment terms
 - Transaction does not make sense (e.g., a machinery company transacting in avocados)
 - Product is inconsistent with the country of export (Panama exporting semiconductors)
 - Lack of knowledge risk—inexperienced bank staff reviewing complex legal documents

Due diligence

In a risk-based program, issuing banks should have documented processes that allow for due diligence based on the perceived risk posed by the customer/transaction. At a minimum, an issuing bank must conduct enough due diligence on the applicant, beneficiary and all FIs involved in order to make a reasonable risk assessment of the transaction. Higher risk transactions will necessitate additional or enhanced due diligence (EDD). This risk assessment of the financial transaction and customer risk will drive the controls put in place to mitigate the risks. FIs should document in trade finance procedures what constitutes a higher risk transaction. FIs may choose to include the following as indicators of higher risk:

- A customer new to the bank
- Higher risk geographies
- Higher risk products, such as weapons, ammunition, chemicals, defense machinery, technical data, nuclear material, gems or other natural resources
- An unusually high dollar amount
- Involvement of the military or police

Foundational due diligence reviews include, but may not be limited to:

- Robust sanctions screening processes to include:
 - Name screening of applicant, beneficiary, intermediary and final FIs, vessels, ports and countries
 - Product screening to ensure the product is permitted to be exported to the receiving country



■ Export controls

- Determine if an export license or permit is required
 - ▲ The product is not a dual-use good—that is, an item that can be used both for civilian and military applications—or otherwise controlled for export. Exports of dual-use, military and controlled goods are severely restricted because they can be classified for civilian use but later be transformed for military use, terrorist use or other nefarious purposes.
 - ▲ Consider all aspects of the international trade transaction, including intangible commodities, such as intellectual property and installed software, which may accompany the export of computers.
 - ▲ Shipments may require a license based on product characteristics, business or intended use by the purchaser, such as a military supplier, and based on the destination country, such as those with high diversion risks or are sanctioned.
- Determine if any parties are denied, debarred or otherwise prohibited from cross-border trade. Ensure that not just sanctions lists are running as part of the screening process but also solely trade-based restriction lists (e.g., U.S. Department of Commerce entity and unverified lists).

■ Anti-boycott surveillance measures

- U.S. regulations prohibit companies and their international offices from complying with economic boycotts that are not approved by the U.S. government. To avoid knowingly or unknowingly participating in prohibited boycott activity, use automated text block screening capabilities to look for keywords that can indicate the presence of boycott activity.

Enhanced reviews may include but are not limited to:

- Checks on the reasonableness of the product prices by matching to current U.S. Census pricing ranges⁸
- Ensure goods financed are reasonable purchases for the parties involved
- Validate commodity and party information contained in the lending documents against the actual transactions documents (transport documents, bills of lading, customs and commercial invoice comparison, contracts, submitted import or export declarations)
- Review validity of website⁹
- In addition to screening the parties named above, banks may also consider screening the logistics companies and any agents or third parties present in the transaction

- Validate export or import licenses with the governmental agency that issued the license
- Use independent or open-source information to validate critical information, such as whether a vessel or party to the transaction has been attached to negative news
- Validate container and seal numbers and/or check shipping vessel International Maritime Organization (IMO) and Maritime Mobile Service Identity (MMSI) numbers against sanctions lists

Controls

In addition to performing customer due diligence and EDD, FIs will want to consider these preventive and detective controls in their trade finance program:


- As per the “Guidance to Address Illicit Shipping and Sanctions Evasion Practices,”¹⁰ jointly issued by multiple U.S. federal government departments/agencies:
 - Implement relevant controls for maritime industry clients, particularly those that own, operate and/or provide services to ships operating in areas determined to pose a high risk for sanctions evasion. Transshipment-based transactions can bring enhanced risk to cross-border trade. Common transshipment points through which controlled exports have historically passed before reaching destinations in Russia or Belarus are Armenia, Brazil, China, Georgia, India, Israel, Kazakhstan, Kyrgyzstan, Mexico, Nicaragua, Serbia, Singapore, South Africa, Taiwan, Tajikistan, Turkey, the United Arab Emirates and Uzbekistan.¹¹
 - Incorporate best practices in contracts related to financial business relationships in the maritime industry.
- Screen shot searches if the search system does not retain for at least 60 months—the axiom applies “If you did not document it, it did not happen.” FIs must be able to prove to examiners and auditors that process steps were followed.
- Consider in what instances a copy of Form BIS-711¹² Statement by Ultimate Consignee and Purchaser will be requested or required. While this can be an important risk mitigation step, if obvious noncompliance and lack of governance or controls within the organization of the signing party are present, Form 711 is insufficient to ensure trade compliance reasonable care standards have been met.
- Ensure the trade finance department has a documented procedure to survey, report and escalate suspicious or unusual activity to those responsible for suspicious activity monitoring and reporting. Recently, the Financial Crime Enforcement Network (FinCEN) and the U.S. Department of

Commerce's Bureau of Industry and Security issued a joint alert urging FIs to be vigilant against efforts by individuals or entities to evade export controls and to reference this alert in suspicious activity report field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "FIN-2022-RUSSIABIS" for transactions involving specific commodities, transshipment points and countries of concern.¹³

- Ensure the trade finance or suspicious activity monitoring/reporting team has procedures in place to report boycott, export and/or economic sanctions violations to the appropriate federal agency.

Due to the multiple types of trade finance transactions, the complexity of the documents and the nonstandardization of supporting documents, it is highly unlikely that compliance reviews will be fully automated. Where there is human intervention, there is a risk of human error. Implementing the following may assist with identifying and/or reducing the human error risk:

- Consider using a checklist to avoid missing steps when the review process steps are not automated.
- Implement a quality assurance process prior to permitting transactions to move forward.
- Ensure appropriate bank employees, including trade finance team members, receive periodic training on TBML risks and controls, economic sanctions and trade embargo risks and controls, and import and export risks and controls. Ensure processes are in place to document the content of the training and the attendees.
- Periodically review trade finance-related policies and procedures. Update as new guidance is distributed.

"The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection."¹⁴ FIs must implement robust controls appropriately risk-based in an effort to identify instances of TBML. Identify the risks for each type of trade finance activity conducted by the FI, then match the controls to those risks. The controls discussed in this article are not appropriate for every trade finance-related activity but can serve as a starting point for banks issuing letters of credit. 

Amy Wotapka, CAMS, BSA and OFAC officer, First American Bank, USA, awotapka@firstambank.com

Anne Marie Lacourse, consultant, Dow Jones Risk & Compliance, USA, annemarie@lacourse.us

- ¹ "Trade Finance Principles," *The Wolfsberg Group, ICC and BAFT*, 2019, <https://iccwbo.org/content/uploads/sites/3/2019/03/trade-finance-principles-2019-amendments-wolfsberg-icc-baft-final.pdf>
- ² "Trade Finance Global 2023," *Trade Finance Global*, <https://www.tradefinanceglobal.com/trade-finance/types-of-trade-finance/>
- ³ "Risks Associated with Money Laundering and Terrorist Financing," *FFIEC*, <https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/19>
- ⁴ "Trade Based Money Laundering," *Financial Action Task Force*, June 23, 2006, <https://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf>
- ⁵ "These 3 charts show how international trade works—and the current state it's in," *World Economic Forum*, October 4, 2021, <https://www.weforum.org/agenda/2021/10/how-international-trade-works-global-economy/>
- ⁶ "What Is ChatGPT? How AI Is Transforming Multiple Industries," *Forbes*, February 1, 2023, <https://www.forbes.com/sites/qai/2023/02/01/what-is-chatgpt-how-ai-is-transforming-multiple-industries/?sh=66dc4f8a728e>
- ⁷ "Black Market Peso Exchange in Money Laundering: Distinctive Characteristics and Definition," *Financial Crime Academy*, <https://financialcrimeacademy.org/black-market-peso-exchange-definition/>
- ⁸ Maritza Torres, "Understanding Verify Messages," *U.S. Census Bureau*, July 12, 2017, https://www.census.gov/newsroom/blogs/global-reach/2017/07/understanding_verify.html
- ⁹ Aaron Drapkin, "How to spot a fake website by reading the URL," *ProPrivacy*, February 14, 2021, <https://proprivacy.com/guides/identify-fake-websites>
- ¹⁰ "Guidance to Address Illicit Shipping and Sanctions Evasion Practices," *U.S. Department of the Treasury, Department of State and U.S. Coast Guard*, May 14, 2020, https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf
- ¹¹ "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," *Financial Crime Enforcement Network*, June 28, 2022, <https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf>
- ¹² Form BIS-711, *U.S. Department of Commerce, Bureau of Industry and Security*, <https://www.bis.doc.gov/index.php/documents/just-licensing-forms/803-bis-711-statement-by-ultimate-consignee-and-purchaser-1>
- ¹³ "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," *Financial Crime Enforcement Network*, June 28, 2022, <https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf>
- ¹⁴ "Risks Associated with Money Laundering and Terrorist Financing," *FFIEC*, <https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/19>

EUROPE EXPRESS

Interested in
knowing what
is happening in
Europe?

Check out our *Europe
Express* column for the
latest industry insights
from subject-matter
experts across Europe.



ACAMS ™



The great divide:

**Getting convergence
right this time**



As the world becomes increasingly interconnected and digital, so too has the threat of financial crime. Traditionally, siloed methods of combating financial crime, such as anti-money laundering (AML) and fraud detection, must adapt to the changing landscape and find ways to effectively mitigate the risks posed by increasingly sophisticated cybercriminals. At the same time, the field of cybersecurity is also evolving due to increased threats, such as phishing schemes and business email compromise, which can lead to the redirection of payments by transnational criminal organizations.

The convergence of AML, fraud and cyber presents both challenges and opportunities for financial institutions (FIs) and law enforcement agencies. On the one hand, it requires the development of new technologies and approaches to identify and prevent financial crime. On the other hand, it also creates the opportunity for greater collaboration and information sharing among stakeholders, allowing for a more comprehensive view of risks posed to the institution.

This article will explore the convergence of AML, fraud and cyber and discuss the challenges and opportunities it presents. It will also examine the role of people, processes and technology in combating financial crime and consider the future of financial crime prevention in the digital age.

Similar, yet different

There is a clear overlap between fraud, AML and cybersecurity, as all three are concerned with protecting clients and the institution against financial crime and other illicit activity. For example, cybercriminals may commit fraud to steal sensitive financial information or launder money to obscure the origin of their funds. Similarly, individuals or organizations involved in money laundering may use cyberattacks to gain access to financial systems or to cover their tracks. Fraud was named as the largest driver of money laundering, generating billions of dollars annually, according to the U.S. Department of the Treasury National Money Laundering Risk Assessment, further highlighting the interconnection.¹

Despite the similarities between fraud, AML and cybersecurity, many previous attempts at convergence have failed. Some of the reasons are found in deep-rooted silos that have developed over the years, creating barriers to transformation. While there is general agreement that convergence drives many benefits, the hurdles can feel overwhelming to overcome.

HURDLES:	BENEFITS:
<ul style="list-style-type: none"> • Siloed data and applications • Required buy-in from organizations with distinct leadership, budgets and operations • Satisfaction with the status quo • Short-term budget restrictions 	<ul style="list-style-type: none"> • Enhanced ability to identify complex financial crimes schemes • Equal access to technologies across domains • Alignment with regulatory expectations • Long-term cost savings

The benefits of the convergence of AML, fraud and cyber

Enhanced ability to identify complex financial crime schemes

As the financial sector becomes increasingly digital, so too does the risk of financial crime. Cybercriminals are constantly finding new ways to exploit vulnerabilities in the system, whether through phishing scams, ransomware attacks or other forms of cybercrime. At the same time, traditional methods of combating financial crime in money laundering and fraud are struggling to keep up with increasingly sophisticated threats that require broader data features and greater collaboration. Criminals exploit these intelligence gaps within FIs for their benefit.

Equal access to technologies and information across domains

Combining resources means that technology investments can be amortized across teams. Access to powerful and automated technology to handle tasks across the intelligence life cycle, from data engineering to model development, visualization and deployment to ongoing monitoring and optimization, is shared by the team. Illicit actors are always looking for the weakest link and will capitalize on it once found. Convergence raises the bar across the board for better defense.

Alignment with regulatory expectations

While regulators have not explicitly mandated convergence, there has been guidance that demonstrates an expectation of information sharing and collaboration. In the U.S., the suspicious activity reporting requirements have expanded in recent years to include mandatory suspicious activity report (SAR) submissions of cyber-events, and the Financial Crime Enforcement Network list of National Priorities emphasizes comprehensive risk management. Greater collaboration across teams also ensures standardized business processes and improved governance for meeting regulatory filing requirements.

Long-term cost savings

There is the redundancy of data, technology and workforce across silos that is increasing the cost of compliance. However, convergence brings long-term cost savings through integration. In a recent survey, LexisNexis found that institutions that invest more in technology transformation have experienced lower costs and fewer compliance operations challenges.²

The hurdles to the convergence of AML, fraud and cyber

Siloed data and applications

Overhauling deeply siloed data and applications can feel overwhelming and requires multi-phased projects to unravel. When embarking on enterprise-scale projects, leaders often struggle with where to start. Creating an inventory of technology and business processes in the current state and a strategy of what the target state will look like is a great start. Convergence is an evolution, so start with applications that have an overlap of data to deliver quick wins to stakeholders.

There are many unknowns when embarking on the convergence journey, but the payoff will improve the ability to manage both risk and operations

Required buy-in from organizations with distinct leadership, budgets and operations

Cooperation across organizations is often harder than it looks. Leadership has different charters, budgets and distinct operations, which require changing deeply entrenched processes. Fraud leaders are concerned with losses and the bottom line. AML leaders are worried about meeting regulatory expectations and mitigating reputation risk. Cyber leaders often have oversight that goes far beyond financial crime into areas such as conduct and physical security. It is essential to have executive sponsorship at a program level as strategies will evolve based on innovations in technology and the threat landscape.

Satisfaction with the status quo

Some leaders pay homage to the old saying, "if it is not broken, do not fix it." Change is disruptive and can evoke fear regarding goals not being aligned, not being able to balance workloads through the technology integration process and/or the impacts it will have on morale. There are many unknowns when embarking on the convergence journey, but the payoff will improve the ability to manage both risk and operations. Ideally, convergence will make investigators' work more impactful by providing them with greater intelligence and context.

Short-term budget restrictions

The World Bank has cited that the global economy will come "perilously close" to a recession due to a slowdown in mature markets such as the U.S., Europe and China.³ In response to this and other economist predictions, FIs are signaling tightened budgets. However, there are steps that can be taken to augment current operations working toward convergence.

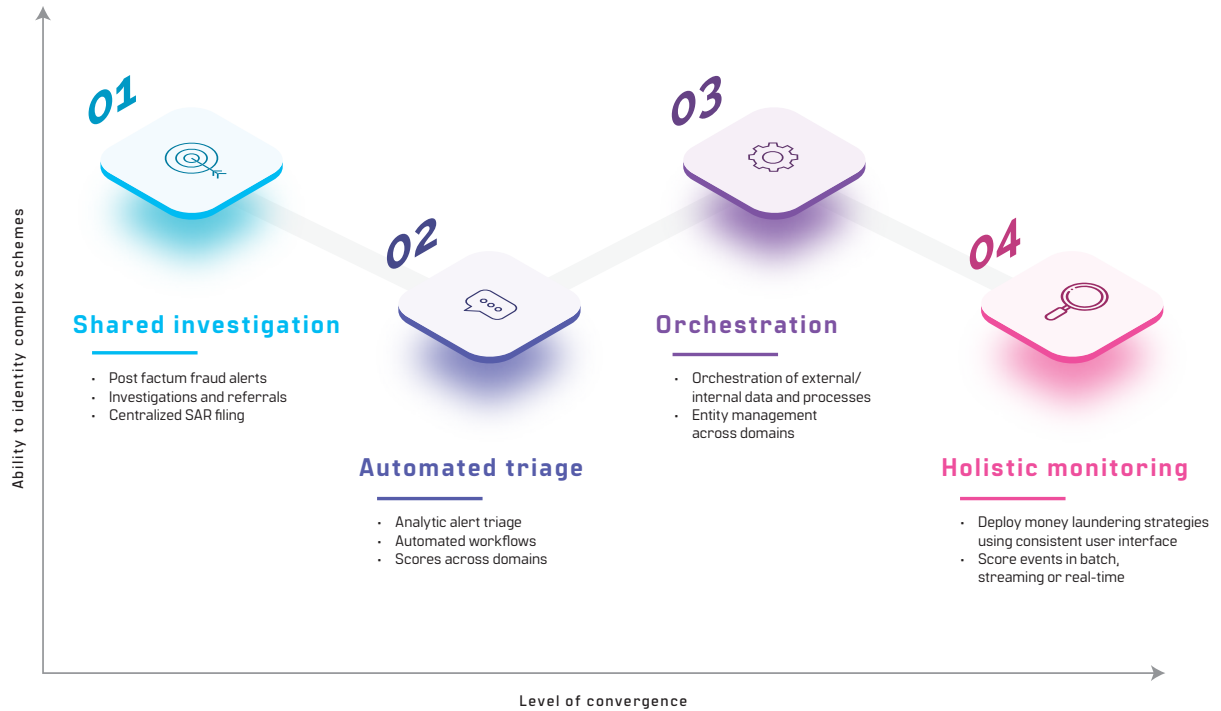
What modern convergence looks like

There are many misconceptions about what convergence looks like, so perhaps the best place to start is to define what convergence is not. Convergence does not look like the following:

- Elimination of specialized experts in fraud, AML and cyber
- Single business process and workflow for all domains
- Common service-level agreements
- One detection engine

Convergence is about bringing people and data together using technology while embracing what each needs to reach quality decisions. This is best illustrated in Graphic 1 by reviewing different operating models that are found in the industry:

Graphic 1: The levels of convergence




Source: SAS

- 1. Shared investigation:** Known fraud events, automated system alerts and manual referrals are collated into a common case management system. If entity management of common party identifiers is lacking, advanced search is a critical requirement. Typically, SARs/suspicious transaction reports (STRs) are filed following centrally governed processes.
- 2. Automated triage:** Discrete detection events are consolidated into a common scoring and prioritization methodology. The ability to score at a party or external party dimension is desirable. Common policies and operating models are governed through automated workflows that improve sharing of information across teams.
- 3. Orchestration:** Through industry-standard application programming interfaces (APIs), external data (adverse media, device reputation, biometrics, etc.) is ingested to supplement profiles and historical data to derive a more complete view of risk exposure. For AML investigators, this can reduce the time it takes to complete an investigation. In fraud operations, orchestration may be used to push step-up authentication or deposit holds based on a series of conditions.
- 4. Holistic monitoring:** As model governance becomes more critical to deploying machine-learning strategies, providing common user experience and methodology is essential. In some cases, the features and algorithms may be designed to identify productive investigations without bias to traditional typologies.

In a 2021 survey, Aite Novarica cited that 42% of FI compliance executives had information and data sharing as well as enterprise policies and processes in place. Furthermore, 27% had fully consolidated case management and staff, while only 23% had integrated detection technology.⁴

Conclusion

The convergence between fraud, AML and cybersecurity is a major challenge for organizations and governments around the world. The lines between financial crime disciplines have blurred due to the sophistication and coordination of transnational criminal organizations. To effectively address these challenges, it is necessary to adopt a comprehensive approach that combines strong technical controls with effective risk management and compliance processes. By working together, we can create a safer and more secure financial system for all. 

Beth Herron, manager, Americas Fraud and Security Intelligence Practice, Beth.Herron@sas.com

David Stewart, director, Financial Services Vertical, Global Security Intelligence Practice, David.Stewart@sas.com

Rob Goldfinger, CAMS, senior SME, Fraud Security and Intelligence Business Development, Rob.Goldfinger@sas.com

¹ "National Money Laundering Risk Assessment," *U.S. Department of the Treasury*, February 2022, <https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf>

² "2022 True Cost of Compliance Study Global Summary," *LexisNexis Risk Solutions*, June 2022, <https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report>

³ "Global Economic Prospects," *The World Bank Group*, January 2023, <https://openknowledge.worldbank.org/bitstream/handle/10986/38030/GEP-January-2023.pdf>

⁴ "Key Trends Driving AML Compliance Transformation in 2022 and Beyond," *Aite Novarica*, February 2022, <https://aite-novarica.com/report/key-trends-driving-aml-compliance-transformation-2022-and-beyond>

THE BIG IMPACTS of small, in-house BMAs: A case study in the fight against corruption

Faced with the challenges imposed by COVID-19 and global economic downturns, what will differentiate strong businesses from weak ones going forward will be their ability to think ahead, adapt and innovate. Fighting corruption and other financial crimes continues to be a huge operational burden and a major pain point for many governments and private institutions, particularly when it comes to investigating and adjudicating underlying criminal activity. For the anti-financial crimes (AFC) industry, not only is the dependence on instinct, critical thinking and experience relevant to tackle complex cases and weather challenging times, but also the ability to create new tools and applications innovatively will go a long way toward running an efficient and ultimately thriving operation.

Historically, businesses have adopted traditional technology implementation to gather, organize and present information. This has proven to be costly over the years. Today, we have what are generally referred to as business-managed applications (BMAs)—in-house tools that help businesses access information and perform basic operations quickly and more accurately. Adoption of BMAs, as described in this article, can provide ideas for “future-readiness” in anti-money laundering (AML) compliance as well as the groundwork for the digital transformation of businesses that allows for the leverage of digital capabilities and innovation to meet business needs while reducing costs.¹

Fighting financial crimes and the corresponding compliance technology needed involves complex methods and technology. As a result, technology professionals are usually seen to be at the forefront of AFC innovation. Consequentially, AFC professionals (such as analysts and investigators) who review alerts and carry out case investigations and research are seen to be at the end of the value chain. However, AFC professionals can become empowered in various ways to become technically inclined and apply their knowledge in developing simple BMAs. Thus, BMAs can become an adaptable solution, integrating seamlessly into existing workflows. In-house BMAs, as demonstrated in the case study below, were found to have multiple advantages, including:

1. Complementarity and alignment with current and future technology-managed applications (TMAs)
2. Quicker identification of pain points and proffering of appropriate solutions that produce immediate results
3. No need for a sudden change in existing workflow or processes, to which staff, customers and regulators are prone
4. Reduction in regulatory, reporting, operational and financial risks
5. Increase in capacity, productivity and operational efficiencies with positive impacts on the bottom line



- 6. A boost in morale and recognition for AFC professionals for doing what is referred to as “great work”² with an overall positive impact on job satisfaction and business results

Case study: Use of in-house BMA tools in combating corruption

Money laundering and corruption are inextricably linked. Money laundering is the process of concealing the origin, ownership or destination of illegally or dishonestly obtained money by hiding it within legitimate economic activities to make them appear legal.³ Corruption, as one of the means of unlawful enrichment, usually involves the abuse of power or trust for private or personal benefit.⁴ Although corruption is a truly global issue, as a continent, Africa underperforms in comparison to the rest of the world. The number one area in which individual African nations ranked lowest in the Basel AML Index⁵ and Financial Action Task Force (FATF) analysis⁶ was bribery and corruption.

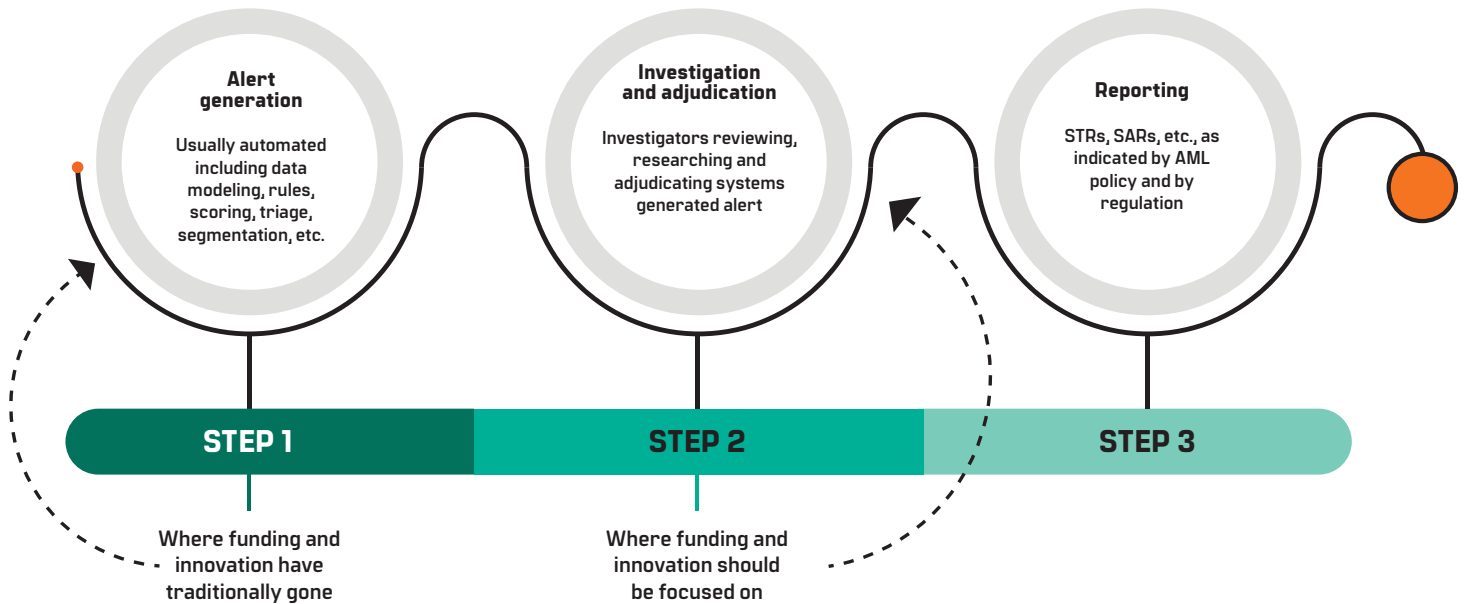
It is estimated that illicit financial outflows from Africa far exceed the Overseas Development Assistance (ODA) that Africa receives annually, thus hindering development efforts and undermining poverty reduction strategies.⁷ As evidence has shown, international funds provided for

public health have ended up being embezzled in the past,⁸ and with the onset of the COVID-19 pandemic, with charitable donations being raised for developing countries impacted by the outbreak, the availability of these charitable funds has meant a higher likelihood of corruption. Criminals may try to bribe government officials, lawyers and employees of financial or non-financial institutions (FIs) to continue running their criminal businesses. It is, therefore, important now more than ever before for corruption to be curbed and mitigated.

Despite the use of advanced AML models, including the implementation of artificial intelligence and machine learning algorithms, the sophistication of corruption and other money laundering activities makes it possible for many such cases to go undetected or unresolved. The most powerful medium of defense remains human investigators. This case study shows that despite the use of transaction monitoring systems (TMS), adjudicating complex cases requires the ability of investigators to develop innovative techniques, such as the creation of BMAs of their own that enhance or complement TMS and other TMAs.

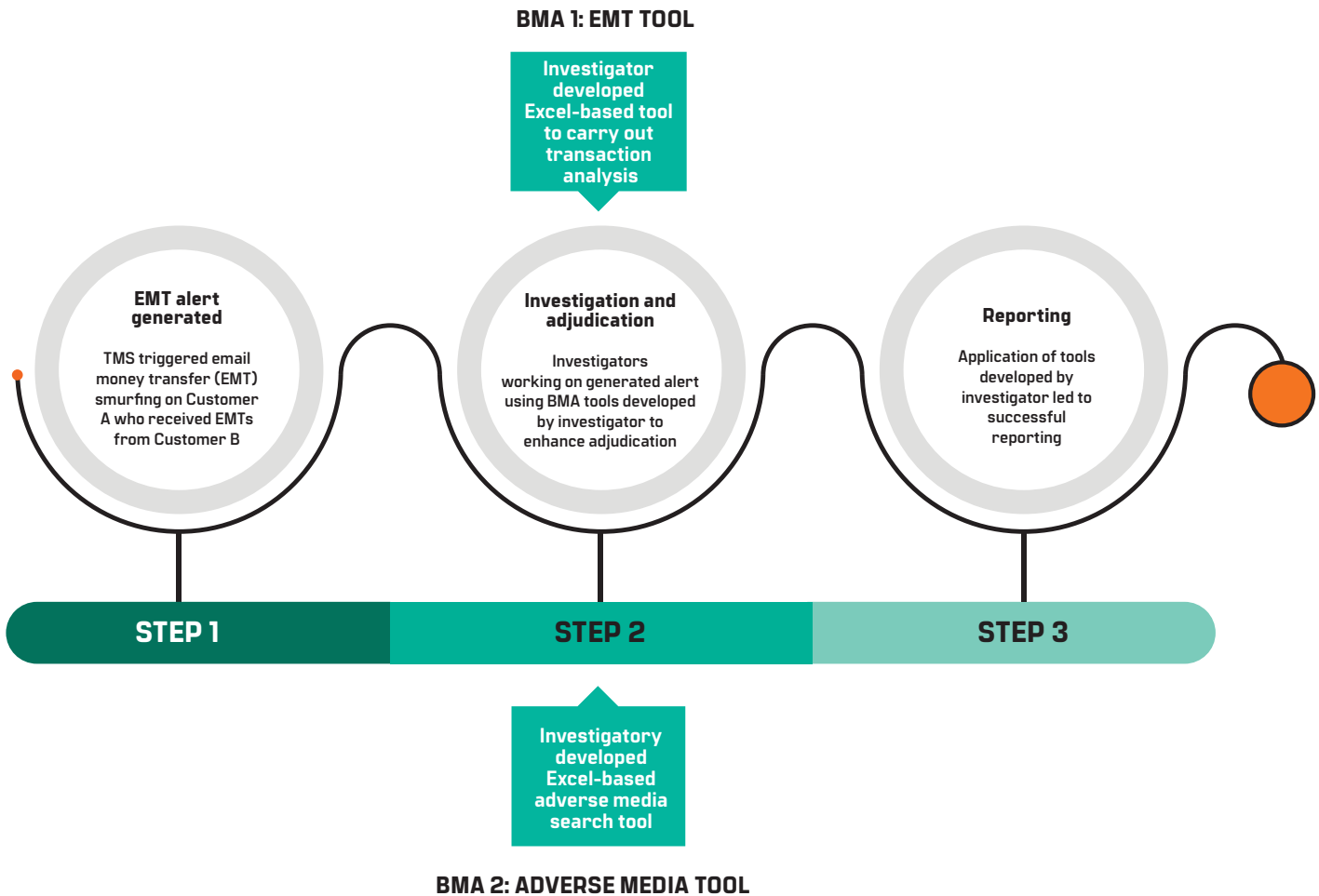
A typical AML investigation follows the three phases shown in Graphic 1.

Graphic 1: The three phases of an AML investigation



Visualization by Solomon Dyeniran and Isaac Tsang

Graphic 2: Alert and reporting process



Visualization by Solomon Oyeniran and Isaac Tsang

In most FIs, the process of alert generation and anomaly detection have received a lot of attention, taking the form of AML data modeling or TMAs, such as TMS. Yet, there is significant work to be done in the second stage of the investigation process. This means that any support this stage receives will ultimately produce a quicker turnaround time for adjudication and reporting, with improved overall quality and efficiency of the investigation process.

Upskilling and enhancing the capabilities of the investigators themselves not only complements the TMS technology but also enhances the investigation process. Unlike a TMS that requires high spending on infrastructure and change management, enhancing the skills of those who do the actual investigating is cost-effective because it requires

less spending. Research has further shown that creating room for such an innovative environment can significantly boost business results.⁹

A case study helps to prove this point more effectively. After a TMS alert was generated, an investigator with basic skills was able to innovate the workflow with two BMAs, as shown in Graphic 2.

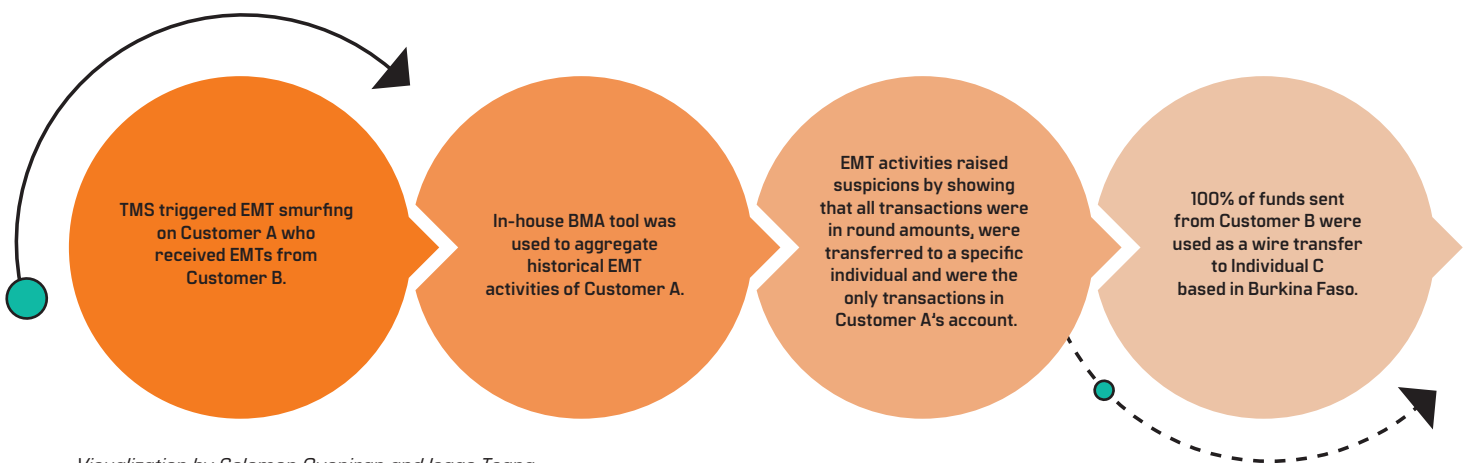




BMA 1: Email money transfer (EMT) tool

A further breakdown of the function of BMA 1 (the EMT tool) is shown in Graphic 3.

Graphic 3: Step-by-step function of BMA 1



Visualization by Solomon Oyeniran and Isaac Tsang

In this example, the TMS captured a portion of the activity that met the scenario threshold. Using the BMA EMT tool allowed the investigator to aggregate transaction data beyond what the TMS indicated and helped establish key networks and players in the activity. In particular, the EMT helped raise the nature of the activity from EMT smurfing to a potential corruption case.

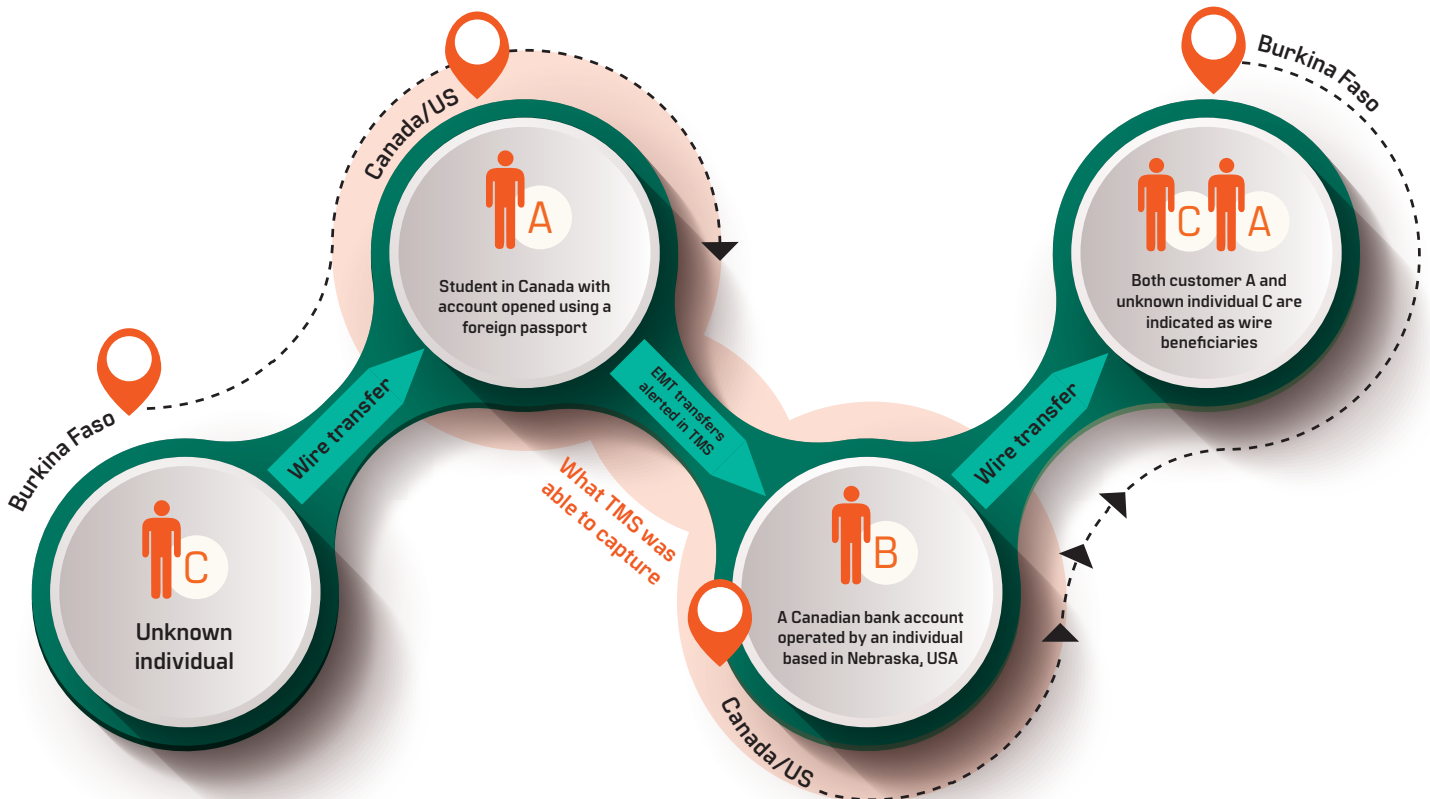
One or two fund transfers do not necessarily raise a dust cloud; it is the aggregation of historical transaction records that makes the difference. This is what the EMT tool was able to do, giving the investigators a clearer path to adjudicating and reporting the case.

BMA 2: Adverse media search tool—open-source intelligence (OSINT)

As part of the 360-degree AML investigation model, understanding the customer includes relevant information (adverse or otherwise) associated with customers, their business and their close associates. In particular, the 360 model suggests the internet OSINT and other database research provide supporting information during an investigation.¹⁰

Building on evidence gathered with BMA 1 (the EMT tool), further investigation into Customer A shows that funds in the account were wire transfers from Individual C, who is based in Burkina Faso—a high-risk jurisdiction. Using BMA 2 for adverse media on the internet related to these individuals provided additional intel on Individual C, indicating involvement as a top government official in Burkina Faso. Customer A received wires from Individual C over the span of one year. There was no other activity in the account of Customer A until funds were used for numerous EMTs to Customer B, which triggered the TMS alert. A full picture of the entire flow of funds is now possible with the help of both BMAs and is shown in Graphic 4.

Graphic 4: The flow of funds



The BMAs in the case study provided a larger scope and effective coverage of the alert generated by TMS.

Visualization by Solomon Dyeniran and Isaac Tsang

The in-house BMA 2 was useful in helping to establish the web of relationships between counterparties. OSINT matching Individual C's name shows Individual C to be a former Burkina Faso politically exposed person. Although the actual source of the funds and the purpose of the initial wire sent by Individual C could not be verified, the allegation of corruption scandals in the local Burkina Faso news implicating Individual C confirmed the activity to be a corruption case. Several local and international newspaper reports captured by the BMA 2 with OSINT showed a spate of corruption that lasted for nearly 30 years.¹¹


Customer A appears to have used a Canadian student account to hold funds before sending them back to Burkina Faso to make the transaction appear legitimate. In addition, Customer A appears to have another account that was funded by large sums of wire transfers from Individual C in Burkina Faso. Another account held by Customer A was predominantly used for personal purchases of luxury items from high-end stores, which appeared unusual.

Multiple suspicious activity reports were filed on Customers A and B as well as on the wire transactions involving Individual C, with suspected corruption/fraud being the predicate offense. The stage of money laundering suspected was layering, structuring and integration. The case was also referred to the bank's anti-corruption office (ACO) for further investigation and escalation. More importantly, customers were placed on bank monitoring systems while further actions were being taken by the ACO.

Managing BMAs

Despite the critical importance BMAs can play, it is important to have a process or control around their development and operationalization. For example, an AFC analyst or investigator spending more time creating BMAs than on the actual investigation is causing more risk than resolving the case. Because of this, developing a guideline or policy around BMA creation would be a good step. Having a team of AFC analysts and investigators to manage the creation of BMAs and set up a central repository would be another good practice, as this would eliminate the duplication of efforts.

Conclusion

With much investigative work going into cracking sophisticated crime schemes, results are often plagued by costly errors and low-quality outcomes. The use of small, in-house BMAs can produce meaningful results in AFC work and the overall impact on the compliance state of the business. This approach could also help organizations succeed in the digital economy by reducing costs through standardizing and automating processes; reusing data, processes and technology; and identifying areas where productivity can be increased.¹² While BMAs look daunting on the surface, the development and deployment of simple in-house BMAs can help fast-track investigation, adjudication and reporting. To mitigate operational risk, address increased regulatory requirements and exercise the effective use of BMAs, it is important to implement a BMA governance framework that aligns people, processes and technology. 

Solomon Oyeniran, CAMS, manager, AML Robotics, Reporting and Automation Solutions, Bank of Montreal, Toronto, Ontario, Canada, solomon.oyeniran@bmo.com

Isaac Tsang, CAMS, senior manager, AML Robotics, Reporting and Automation Solutions, Bank of Montreal, Toronto, Ontario, Canada, isaac.tsang@bmo.com

Note: The information contained in this article is the opinion of the authors and does not reflect the policies, procedures, or opinions of the authors' employer or associations of which he is a member.

- ¹ Stephanie Woerner, Peter Weill and Ina Sebastian, "What it means to be a 'future-ready' firm," *MIT Sloan School of Management*, October 19, 2022, <https://mitsloan.mit.edu/ideas-made-to-matter/what-it-means-to-be-a-future-ready-firm>
- ² Gary Beckstrand, "Employee engagement is out. Here's a better metric," *Fast Company*, February 8, 2022, <https://www.fastcompany.com/90719359/employee-engagement-is-out-heres-a-better-metric>
- ³ "Anti-money laundering in West Africa," *Transparency International*, <https://www.transparency.org/en/projects/anti-money-laundering-aml-in-west-africa>
- ⁴ "What is corruption?" *Transparency International*, <https://www.transparency.org/en/what-is-corruption>
- ⁵ "Basel AML Index: 8th edition. A country ranking and review of money laundering and terrorist financing risks around the world," *Basel Institute on Governance*, August 2019, <https://baselgovernance.org/sites/default/files/2019-10/Basel%20AML%20Index%208%20edition.pdf>
- ⁶ "Countries," *Financial Action Task Force*, <https://www.fatf-gafi.org/countries/>
- ⁷ "Anti-money laundering in West Africa," *Transparency International*, <https://www.transparency.org/en/projects/anti-money-laundering-aml-in-west-africa>
- ⁸ Ngozi Okonjo-Iweala, "Corruption: Myths & Realities In a Developing Country Context, The Second Annual Richard H. Sabot Lecture," *The Center for Global Development*, p. 5, June 2007, <https://www.cgdev.org/publication/corruption-myths-realities-developing-country-context>; Muhammad Akram, Asim Nasar and Abid Rehman, "Misuse of charitable giving to finance violent extremism: A futuristic actions study amidst COVID-19 pandemic," *Social Sciences & Humanities Open*, Volume 4, Issue 1, 2021, <https://www.sciencedirect.com/science/article/pii/S259029112100036X?via%3DIuh>
- ⁹ For more information on the capital expenditures and operating expenses that can be saved: Gary Beckstrand, "Employee engagement is out. Here's a better metric," *Fast Company*, February 8, 2022, <https://www.fastcompany.com/90719359/employee-engagement-is-out-heres-a-better-metric>; "Engagement Revisited: Global Culture Report 2022," *O.C. Tanner*; 2021, <https://www.octanner.com/global-culture-report/2022/engagement-revisited.html>
- ¹⁰ Peter Warrack, "An Introduction to the 360 Degree AML Investigation Model," *ACAMS Today*, June 30, 2017, <https://www.acamstoday.org/introduction-360-degree-aml-investigation-model/>
- ¹¹ "Burkina Faso Mining Lost \$1 Billion to Graft in Decade: Parliament," *Reuters*, October 26, 2016, <https://www.reuters.com/article/us-burkina-mining-corruption-idUSKCN120200>
- ¹² Stephanie L. Woerner, Peter Weill and Ina M. Sebastian, "Future Ready: The Four Pathways to Capturing Digital Value," *Harvard Business Review Press*, 2022, p. 6, <https://hbsp.harvard.edu/product/10564-PDF-ENG>





the RISE of real estate money laundering

The growth of real estate money laundering has been prevalent throughout the past 15 years as the U.S. continues to see ever-changing criminal strategies that facilitate illicit funds to move through the financial system with real estate purchases. As many bank compliance professionals can attest, the regulatory environment has made significant strides to establish strong institutional controls over the movement of funds and bank-facilitated transactions.

Despite rigorous controls in place to safeguard against this activity, money launderers continue their efforts to evade them. In addition, the real estate industry does not always have the same equivalent controls in place, allowing for instances where it is easily susceptible to illegal acts.

This article aims to summarize the emerging risks and the regulatory landscape affecting real estate money laundering, as well as the efforts needed to enhance the controls across the real estate industry.

Global real estate money laundering in 2023

Many studies and reports have quantitatively summarized the global impact of real estate money laundering. Overall, these statistics illustrate that the global impact of this laundering tactic in 2023 is significant. Global Financial Integrity published a report in late 2021 with the following statistics illustrating the impact in the U.S.:

- "From cases reported in the last five years, more than \$2.3 billion has been laundered through U.S. real estate, including millions more through other alternative assets, like art, jewelry and yachts.
- The U.S. remains the only G-7 country that does not require real estate professionals to comply with anti-money laundering (AML) laws and regulations.
- Over 50% of the reported cases in the U.S. involved politically exposed persons (PEPs).
- Commercial real estate [was] featured in more than 30% of the cases and generally had significantly higher values than the residential real estate involved.
- The U.S. has yet to create any reporting obligations for risks in the sector.
- Eighty-two percent of U.S. cases involved the use of a legal entity to mask ownership, highlighting the importance of implementing a robust beneficial ownership [control structure]."¹

The concentrations of PEPs indicate the problematic nature of this laundering method, given the limited guidance by the Financial Crime Enforcement Network (FinCEN) on PEPs involved in real estate.

The question is whether the criminal would ever need to divest from the real estate purchases once the origin of funds is disguised

Real estate involvement in the money laundering cycle

Often, criminals will look for ways to engage in all-cash transactions to the extent that their illicit funds can be spent. These same criminals will look to pay with cash for properties under the market value without needing a bank loan. They often take a loss as the "cleaning" costs for transferring their illegal funds into funds that appear "clean," having bought and sold real estate in a given jurisdiction. In other instances where the illicit funds are layered to some extent already, real estate may serve as the final "integrating" financial asset and will then be held. Real estate integration offers a way to conceal illicit funds with relatively few questions asked.

The question is whether the criminal would ever need to divest from the real estate purchases once the origin of funds is disguised. If you were a money launderer, would you not rather quietly "hide" the illicit proceeds in plain sight and use the property for personal gain? The benefits of this particular method of money laundering include the following:

- Evading sanctions and embargoes
- Committing tax fraud/evasion in various jurisdictions
- Hiding drugs and illicit funds through tangible assets
- Obtaining a legitimate tangible asset with a "clean" appearance from "dirty" proceeds
- Having the ability to generate legitimate income from real estate properties²

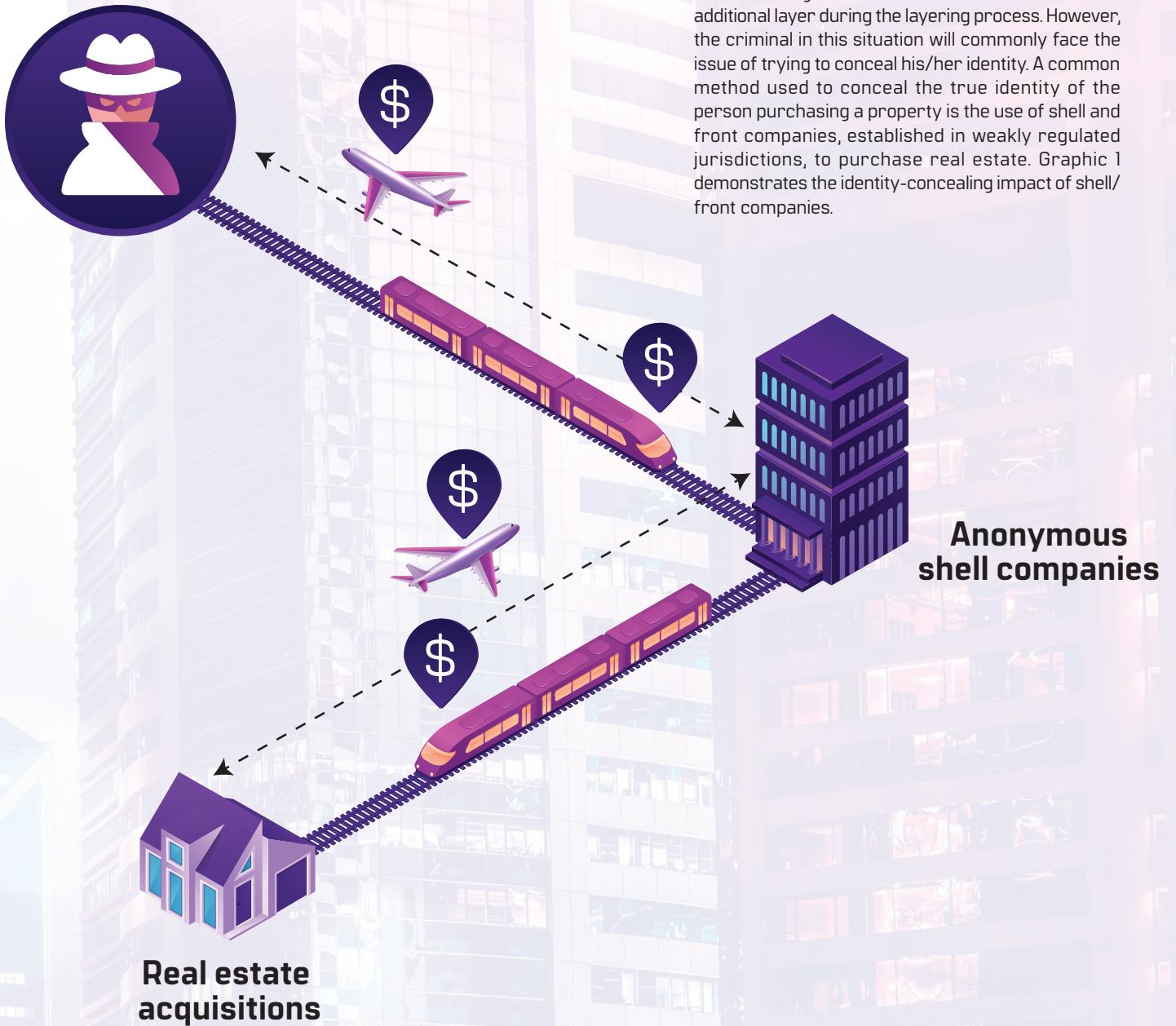
The following examples represent primary strategies used by criminals and money launderers:

- Purchase of a house to renovate and "flip" or resell for a higher price. The investment in property is made with illicit funds, and then the profits become clean.
- Loan backs: Loan money to an individual who pays the loan (mortgage) back with the correct documentation. Red flags would not be triggered with a "clean" identity as the primary owner/borrower.
- The significantly overvalued purchased property is then resold at a cheaper price. The criminal takes the loss, but the sales price comes out clean. The losses are basically the "cost of cleaning funds."
- Qualifying for a loan using a company to conceal ownership and using illegal funds to make the loan payments.
- Using a family member with no criminal record to buy property when they are not the true beneficial owner.

Shell companies to conceal identities

Using illicit funds to buy real estate can serve as a final investing destination for criminals or add an additional layer during the layering process. However, the criminal in this situation will commonly face the issue of trying to conceal his/her identity. A common method used to conceal the true identity of the person purchasing a property is the use of shell and front companies, established in weakly regulated jurisdictions, to purchase real estate. Graphic 1 demonstrates the identity-concealing impact of shell/front companies.

Graphic 1: The impact of shell/front companies

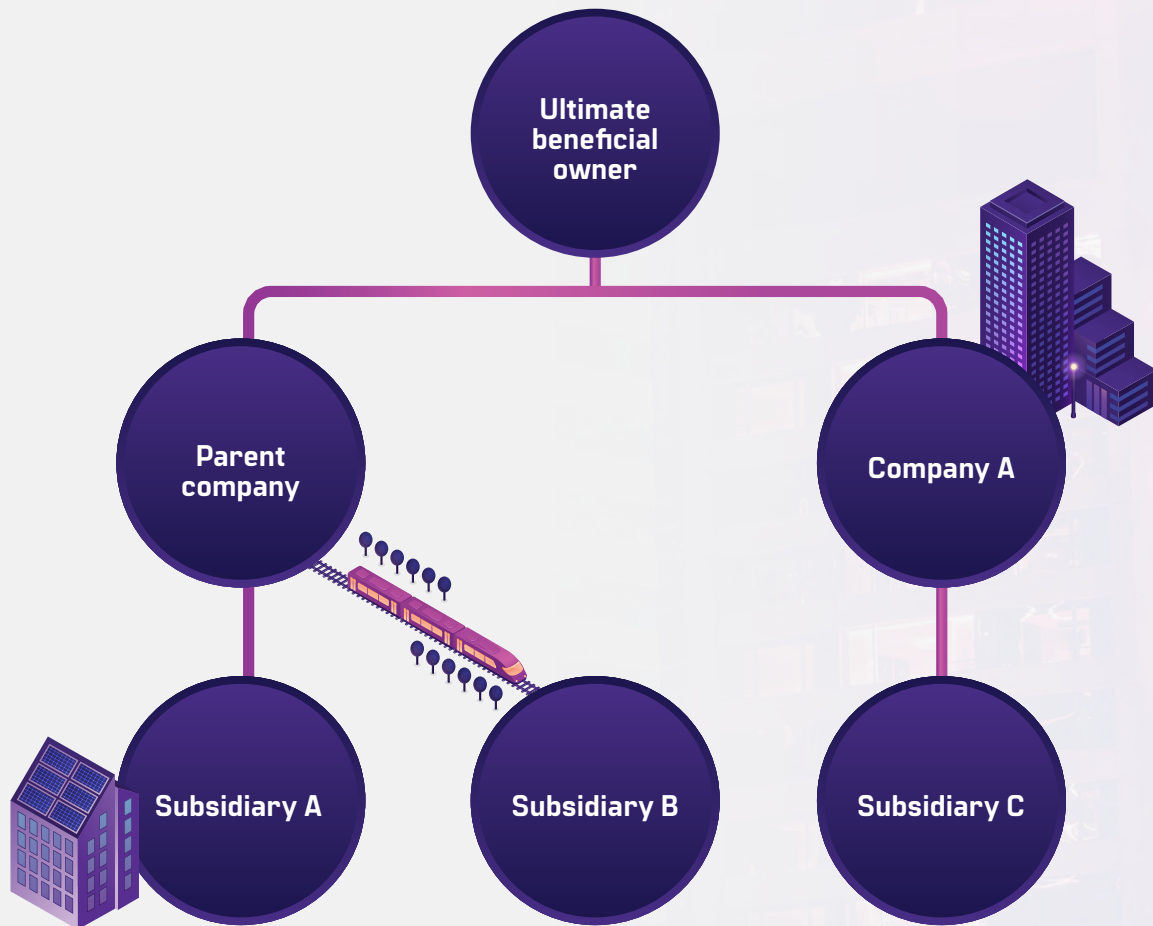


Source: Linkurious³

In 2015, *The New York Times* estimated that shell companies purchased almost half of U.S. residential real estate priced over \$5 million.⁴ The role that these legal strategies assist in hiding illegal funds cannot be ignored when assessing the overall impact of real estate money laundering. Beneficial ownership identification at the institutional level is critical in identifying the true names/parties behind companies/transactions.⁵ Throughout Bank Secrecy Act (BSA) departments across the country,

regulators and individual programs emphasize the importance of identifying beneficial owners. It is essential that compliance staff are educated on how to successfully perform due diligence to reveal the ownership structure prior to accounts being opened and transactions being processed. This type of detailed due diligence is essential in the real estate industry as well if this type of laundering is to be discouraged. Graphic 2 demonstrates a model of the traces leading back to the beneficial owner.

Graphic 2: Beneficial owner structure



Visualization by DJ Antonacio



Red flags

When assessing real estate transactions involving the banking system or occurring in general, compliance professionals and LE commonly look to identify the following red flags:

- Anonymous owner or convoluted buyer representation with a complex ownership structure
- Primary involvement of shell company or trust
- Cash intensive businesses
- Use of intermediaries not subject to AML regulations
- PEPs
- Selling prices significantly lower than the market value
- Location of the property far from the buyer in proximity
- Regions lacking intense AML regulations
- Large amounts of cash utilized for financing

Beneficial ownership identification at the institutional level is critical in identifying the true names/parties behind companies/transactions

Impact of Russian sanctions

The impact of Russian sanctions turned quickly into a “hot topic” from 2022/2023 advisory services, specifically in banking. Particularly, the frequency and complexity of Russian sanctions are reflected in published watch lists, including the Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons (SDN) list.⁶ The consequences of the Russia-Ukraine war left many Russian oligarchs and known associates placed on the SDN list. Many of these individuals were subject to property seizure across the world. U.S. banks have attempted to adapt to ensure that control structures align with the most recently published listings. However, many instances are still noted where Russian parties/funds have made their way into the U.S. or U.K. real estate market:

- The International Consortium of Investigative Journalists (ICIJ) stated that they, “Found that Ukrainian oligarch Ihor Kolomoisky, whose case is cited in GFI’s report, amassed a Midwest real estate empire with his associates, at one time becoming Cleveland’s largest commercial landlords, and leaving behind a trail of unpaid property taxes, unemployed workers and dangerous factory conditions. Kolomoisky has since been sanctioned by the U.S. State Department.
 - Ihor Kolomoisky and associates purchased 22 properties between 2006 and 2015, mostly through companies registered in Delaware. More than \$490 million was siphoned from PrivatBank, a Ukraine bank Kolomoisky owned, toward the purchase of some of these properties.”⁷
- Transparency International U.K. has been collating information on questionable funds from around the world being invested in U.K. property since 2016. This figure now stands at 6.7 billion euros. Of this total, 1.5 billion euros worth of property was bought by Russians accused of corruption or with links to the Kremlin.⁸

Statistics like these demonstrate why some compliance professionals now consider the U.K. and the U.S. as global hubs for money laundering.⁹ Many sources also claim that Russian money has been “pouring” into the U.S. real estate market over the past 20 years.¹⁰ It is often discussed that the USA PATRIOT Act, arguably the most influencing and lasting piece of legislation to combat money laundering throughout the financial system, pushed illicit money from foreign countries to shift into real estate and tangible assets. The reason for this was that the increased regulation over major bank transactions that followed 2001 presented real estate as a less risky alternative to launderers.

In addition, areas with a heightened risk of real estate money laundering concentration have emerged within the U.S.



- The *Miami Herald* reported that in 2015, 53% of all Miami-Dade County home sales and 90% of new construction were cash deals.
- FinCEN issued a Geographic Targeting Order (GTO) for Manhattan and Miami that requires agents and affiliates to report on beneficial owners for purchases exceeding a certain threshold.

Efforts to comply and reform have been initiated, such as FinCEN's issuance of GTOs in 2016 requiring insurance companies to collect and report information on all persons involved in real estate transactions costing over a certain amount. Efforts like this are put in place specifically to identify true owners behind shell companies.

What real estate businesses can do

Adopt AML programs

The solution lies in AML programs being diligently adopted across the real estate sector. For real estate businesses to successfully coordinate and adopt AML standards, they must ensure that they ultimately know the true party behind the real estate transaction. Real estate businesses must adopt a formal AML program detailing the following:

- Risk-based assessment of customers (buyers/beneficiaries)
- A designated officer with AML responsibilities
- Screening for PEPs
- Verification of funding source
 - For example, obtaining bank statements and proof of income, or
 - A published salary for a PEP
- Beneficial ownership registers
 - For example, an entity purchaser verifying the ultimate individuals with ownership interests
- OFAC sanctions screening of all owners/beneficiaries
- Record retention of customers/buyers/related parties

The above practices, if adopted according to AML standards, can reduce the risk of true buyers/beneficiaries being unknown to the real estate business involved in a transaction. As with banking, the level of controls in place will only be as strong as the program's requirements and efforts to apply the standards for each transaction.

Legislation

- There is legislation from 2020 from the U.S. Congress empowering the U.S. Department of the Treasury to stop tax evaders, terrorists and other financial criminals from using anonymous shell companies to facilitate money laundering through real estate.¹¹
- Due diligence of customers under the PATRIOT Act is extremely relevant here, in addition to the AML scrutiny of property transactions.

In December 2021, FinCEN proposed an "Advance Notice of Proposed Rulemaking" to deal with "all-cash" deals that do not require real estate professionals to identify customers, monitor transactions and report suspicious behavior when cash is used. These proposed rules also cover when a mortgage is not utilized by a bank. Requirements similar to the above enhance AML record-keeping responsibilities for all involved in real estate transactions.

Conclusion

Moving forward, the goal at the institutional level as well as the real estate professional level should be to increase the level of transparency and coordination between the two industries. Banks should work with reputable mortgage companies, real estate agents and real estate professionals with AML programs in place. Increased transparency between industries (real estate, insurance, banking, etc.) is the key to successful due diligence on uncovering true owners and real estate laundering schemes. As part of these programs, the real estate industry also must ensure to adopt the practice of screening using sanctions lists.

Bankers can remember that in instances where coordination among members of a real estate transaction is limited, it is essential to “lean” on traditional detailed customer due diligence and know your customer to ensure all parties involved in a transaction are known and reviewed. In addition, when regulatory guidance is lacking, the bank’s policies/procedures set the standard. **AT**

Donald “DJ” Antonacio, CPA, CAMS, managing director, Verittas Risk Advisors, Miami and Tampa, FL, donald.antonacio@verittas.com

- ¹ “Acres of Money Laundering: Why U.S. Real Estate is a Kleptocrat’s Dream,” *Global Financial Integrity*, August 2, 2021, <https://gfhintegrity.org/report/acres-of-money-laundering-why-u-s-real-estate-is-a-kleptocrats-dream/>
- ² Stefano Siggia, “How is real estate used for money laundering?” *Pideeco*, May 18, 2022, <https://pideeco.be/articles/how-is-real-estate-used-money-laundering-aml/>
- ³ “Towers of cash: investigating money laundering through real estate,” *Linkurious*, August 12, 2022, <https://linkurious.com/blog/real-estate-money-laundering/>
- ⁴ Louise Story and Stephanie Saul, “Stream of foreign Wealth Flows to NYC Real Estate,” *The New York Times*, February 7, 2015, <https://www.nytimes.com/2015/02/08/nyregion/stream-of-foreign-wealth-flows-to-time-warner-condos.html>
- ⁵ For guidance on beneficial ownership information, please visit: “Guidance on Obtaining and Retaining Beneficial Ownership Information,” *Financial Crimes Enforcement Network*, March 5, 2010, <https://www.fincen.gov/resources/statutes-regulations/guidance/guidance-obtaining-and-retaining-beneficial-ownership>; For information on beneficial ownership requirements, please visit: “Beneficial Ownership Requirements for Legal Entity Customers—Overview,” *FFIEC*, <https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/03>
- ⁶ Frequently Asked Questions: Specially Designated Nationals (SDNS) and the SDN List, *U.S. Department of the Treasury*, <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1631>
- ⁷ Sean McGoe, “A Kleptocrat’s Dream: US Real Estate A Safe Haven for Billions In Dirty Money, Report Says,” *International Consortium of Investigative Journalists*, August 10, 2021, <https://www.icij.org/investigations/fincen-files/a-kleptocrats-dream-us-real-estate-a-safe-haven-for-billions-in-dirty-money-report-says/>
- ⁸ “Stats Reveal Extent of Suspect Wealth in UK Property and Britain’s Role as Global Money Laundering Hub,” *Transparency National UK*, February 18, 2022, <https://www.transparency.org.uk/uk-money-laundering-stats-russia-suspicious-wealth>
- ⁹ Stefano Siggia, “How is real estate used for money laundering?” *Pideeco*, May 18, 2022, <https://pideeco.be/articles/how-is-real-estate-used-money-laundering-aml/>
- ¹⁰ “Russian money flows through U.S. real estate,” *Criminal Investigations and Network Analysis*, April 22, 2022, <https://cina.gmu.edu/russian-money-flows-through-u-s-real-estate/>
- ¹¹ H.R. Res. 6395, 116th Cong. § 6003 (2020), *U.S. Congress*, <https://www.congress.gov/bill/116th-congress/house-bill/6395>



Choppy waters:

Negotiating the complexities of sanctions due diligence in an uncertain world

In the not-too-distant past, a large international financial institution (FI) was weighing a golden opportunity. It was asked to provide funding for a sizeable manufacturing project in Central Asia. The project appeared sustainable and well-placed to offer a solid return on investment.

However, the venture was being undertaken by a consortium that included a sprawling Russian conglomerate. And in light of the geopolitical context and sanctions imposed by the U.S., the European Union (EU) and their partners following Russia's illegal annexation of Crimea, the FI's compliance department was nervous.

The client had checked the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list and the EU's consolidated

list of restrictive measures on Russia; none of the Russian conglomerate's major shareholders were designated or under sectoral sanctions. Nevertheless, there were whispers that its minority shareholders might be designated or about to be designated, and some directors were politically exposed persons (PEPs). Several affiliated individuals were included in the U.S. Department of the Treasury's 2018 oligarchs list.

This is an example of the complexities associated with sanctions risk assessment. The following article demonstrates how the sanctions risk around this potentially lucrative opportunity—which, because of strict liability, could expose the client to civil or criminal penalties—could be addressed and mitigated by implementing an adequate sanctions due diligence (SDD) process.



SDD: One size does not fit all

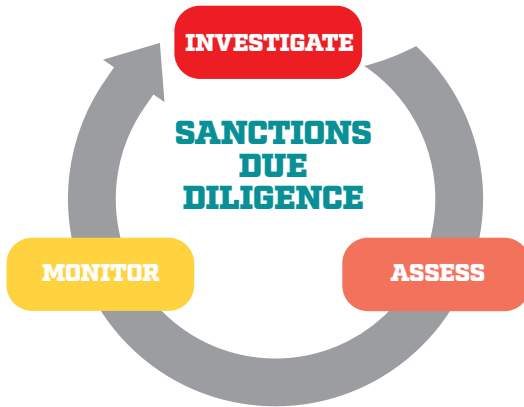
In guidance issued in May 2022, the EU Commission recommended a risk-based approach to sanctions compliance involving a risk assessment, multi-level due diligence and ongoing monitoring. However, it also noted that it was the responsibility of individual firms to decide how their own sanctions compliance programs should look, with “due diligence calibrated according to the specificities of their business and the related risk exposure.”¹ The scope of due diligence thus should be tailored and proportional to the risk.

Companies should regard SDD as a necessity when considering cross-border transactions, particularly in jurisdictions that pose heightened sanctions risk or with partners that have a heightened risk profile—whether because of their geography, the sector they are operating in, the type of activity they are engaged in, the complexity of their structure or difficulties in identifying ownership.

Returning to the proposed Central Asian manufacturing project, the sanctions risk inherent in such a venture would have been considered significant, even prior to Russia’s full-scale invasion of Ukraine in February 2022, making it an obvious target for enhanced SDD. But where does the FI start?

Although there is no one-size-fits-all methodology, SDD must answer a series of fundamental questions that are comparable to traditional anti-money laundering (AML) due diligence and KYC processes, namely: Who is your customer, what do they do and where do they operate? The information must then be checked for existing and potential sanctions exposure and assessed on the basis of the aggregated risks across the entire project. The SDD on the proposed Central Asian project would be broken down into three main steps, as shown in Graphic 1.

Graphic 1: Three main steps in the SDD for the proposed Central Asian project



Visualization by Vlada Tkach and Verena Horne

Source: Berlin Risk Advisors GmbH

Step one: Investigate

With a project of this complexity—involving a consortium that includes a large conglomerate registered in a high-risk jurisdiction—a sensible model would collect data on legal and reputational sanctions risk based on the following four groups of factors identified as contributing to increased overall risk exposure.

Business operations

Determining the extent of existing sanctions exposure through business operations not only covers the obvious first-level checks but is also a key factor in establishing whether the target entity or individual is already on the radar of bodies involved in identifying sanctions targets, such as OFAC, the EU Council and the United Nations.

An assessment of the Central Asian project would therefore include clarifying the sanctions risk exposure associated with the operations of its corporate shareholders and, in particular, the Russian shareholder, as well as the sectors in which they operate. For instance, have they already been targeted by sanctions or could they be in the future? The investigation would then trace and map the existing business relationships of all companies involved in the project to identify the geographical scope of risk exposure and any partnerships with individuals or entities subject to sanctions or at risk of designation. This process would also include screening these companies' managers or directors to clarify if any have been designated or accused of sanctions violations in the past.

Ownership

Determining beneficial ownership of target entities is crucial for SDD due to OFAC's 50 Percent Rule. In most cases, companies are automatically slapped with sanctions in the U.S. and the EU if aggregate ownership by one or more SDNs reaches 50 percent. Even if the rule does not apply, shareholders that are designated, or have been accused of violating international sanctions, contribute to a higher risk of future designation.

This step would therefore focus on determining whether shareholders or ultimate beneficial owners of companies involved in the Central Asian manufacturing project had been designated under national or international sanctions programs, had ties with sanctioned entities or individuals, or had been accused of or convicted for violating sanctions.

This process can be challenging. Shareholders and ultimate beneficial owners may be hidden through complex corporate structures, proxies or legal loopholes in jurisdictions lacking transparency. Moreover, a recent privacy ruling has made the work of identifying company ownership more challenging for third parties. Last November, the EU Court of Justice invalidated the right to public access to beneficial ownership registers recommended as part of the EU's Fifth AML Directive, causing several countries to immediately restrict access to their transparency registers, including Benelux countries, Austria and Germany.²

As such, this step requires specialists with the ability to decipher multi-layered corporate structures who also possess familiarity with the latest tactics employed by sanctions evaders.

Shareholders and ultimate beneficial owners may be hidden through complex corporate structures, proxies or legal loopholes in jurisdictions lacking transparency

Political risk

Political exposure is another critical factor determining whether a person or entity will be designated. Sanctions imposed by the U.S., the EU and the U.K. in the wake of the annexation of Crimea in 2014 and the Russian war on Ukraine in 2022 have specifically targeted members of the Russian political elite and Russian government officials, individuals close to Russian President Vladimir Putin and state-owned enterprises.

This step would therefore assess the political exposure of the Central Asian subject entity and its shareholders and managers, with a particular focus on the Russian stakeholder and its owners.

In addition to identifying current and former PEPs, the process would examine links to political parties, state institutions and security/intelligence services, as well as any allegations of involvement in other states' domestic politics, which would clearly heighten the risk of future designation.

Overall track record

It might seem obvious, but an entity or individual that has been involved in criminal conduct, regulatory violations or unethical business practices would be more likely to be prepared to ignore or deliberately circumvent sanctions. This means it would be important to determine whether target individuals or entities or their shareholders or managers had any serious issues of concern attached to their reputation and track record that would have been likely to put them on the radar of law enforcement and sanction-imposing bodies.

Step two: Assess

As in any due diligence investigation, the above factors must be recorded and analyzed by means of a combination of open-source research—including adverse media and public record database screening—and discreet inquiries with trusted human sources who are experts in the sector, country and sanctions risks. Yet, while the questions and process might be similar to traditional due diligence investigations, the risk analysis stemming from the results will differ for SDD. For example, a location identified as key to the supply chain might be considered low-risk for AML but high-risk from a sanctions perspective.

More often than not, you have to contend with complex structures designed to obscure the identity of beneficial owners—many of whom are skillful in avoiding being identified—and then understand how to apply sanctions rules to entities and individuals with whom you are engaged or planning to be engaged.

This reference to the application of sanctions rules highlights the importance of a reliable methodology to assess the overall aggregate risk inherent across the above four categories. SDD specialists are best placed to help with this daunting task, having tried and tested in-house risk analysis tools that might include specially designed questionnaires and risk-rating models.

The next stage is to consider the results of the SDD as part of a company's overall risk analysis. The ultimate decision will be informed by the company's risk appetite, including taking into account—in the likely case of our Central Asian project—any additional reputation or integrity concerns.

Step three: Monitor

As far as it is possible, the aim of SDD on new deals and partnerships is to future-proof businesses from the legal and reputational risks associated with sanctions and related violations; however, this is a process.

Once a deal or investment has been given the go-ahead, SDD requires ongoing monitoring to identify emerging risks, especially amid the rapidly evolving sanctions landscape. Moreover, companies need to be aware of the potential for issues that are identified as reputational in the initial due diligence investigation to develop into legal risks in the future.

It is, of course, impossible to fully account for a black swan event like the invasion of Ukraine by Russia, which would have triggered immediate legal and reputational concerns and have quickly soured the Central Asian manufacturing project. (Its real-life prototype did go ahead at the time.) Nevertheless, undertaking thorough SDD on prospective partners, as part of a comprehensive risk assessment, can help minimize those risks that are possible to predict.

Outlook

Sanctions compliance programs can also help assess which countries, sectors and companies might be vulnerable to designation or sectoral sanctions in the future. Because if one thing is certain, it is that sanctions have become the foreign policy tool of choice for the U.S., the EU and their allies.

Reluctance among European nations to back blanket restrictions on Russian energy exports before they secure alternative sources underscores the collateral risks associated with the imposition of sanctions in a highly integrated global economy. Nevertheless, the U.S. has reportedly been evaluating a package of economic sanctions against China to deter it from military action against Taiwan, while Taipei has been lobbying the EU to consider similar measures.³ Amid the February spy balloon controversy and senior U.S. military officials anticipating a U.S.-China military conflict by 2025, tightly targeted sanctions against strategic Chinese sectors—such as semi-conductors and telecommunications—cannot be ruled out.⁴

Against this highly uncertain and tense geopolitical context, companies would do well to prioritize the implementation of tailored SDD to help them negotiate the choppy waters of sanctions compliance. **AT**

Vlada Tkach, managing partner, Berlin Risk Advisors GmbH, Frankfurt am Main, Germany, vlada.tkach@berlinrisk.com

Verena Horne, senior consultant, Berlin Risk Advisors GmbH, Berlin, Germany, verena.horne@berlinrisk.com

¹ See EU note on "Circumvention and Due Diligence" accessible through the following platform (bottom of page): https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine/frequently-asked-questions-sanctions-against-russia_en

² "EU Court of Justice Delivers Blow to Beneficial Ownership Transparency," *Transparency International*, November 22, 2022, <https://www.transparency.org/en/press/eu-court-of-justice-delivers-blow-to-beneficial-ownership-transparency>; Carsten Volkery and Volker Votsmeier, "A gift for Putin's friends"—How an ECJ ruling complicates the search for oligarchic assets," *Handelsblatt*, December 5, 2022, <https://www.handelsblatt.com/politik/deutschland/transparenzregister-ein-geschenk-fuer-putins-freunde-wie-ein-eugh-urteil-die-suche-nach-oligarchen-vermoegen-erschwert/28847958.html>

³ "U.S. considers China sanctions to deter Taiwan action while Taipei presses EU," *EURACTIV*, September 13, 2022, <https://www.euractiv.com/section/eu-china/news/us-considers-china-sanctions-to-deter-taiwan-action-while-taipei-presses-eu/>

⁴ "U.S. four-star general warns of war with China in 2025," *Reuters*, January 28, 2023, <https://www.reuters.com/world/us-four-star-general-warns-war-with-china-2025-2023-01-28/>

CAMS



Become a specialist in anti-money laundering with CAMS - the gold standard in AML certification among compliance professionals worldwide.

www.acams.org/cams



Edwin W. Harris Jr.:

Eradicating corruption in West Africa

A *CAMS Today* interviewed Edwin W. Harris Jr., CAMS, director general of the Intergovernmental Action Group against Money Laundering in West Africa (GIABA), a role he assumed on August 1, 2022. Harris holds a master's degree in public administration from Northeastern University, a Master of Business Administration degree from Strayer University and a Bachelor of Science in Economics and Political Science from the University of Liberia.

Harris has over 16 years of progressive experience in the public and nonprofit sectors. He has in-depth knowledge and skills in governance, transparency and financial crimes. He has relevant skills on issues relating to governance in the fight against money laundering, the formulation of policies and the implementation of anti-corruption strategies.

As a firm believer in using accountability as a tool to adopt remedial measures to prevent reputational risks for the institution and staff, Harris talked to *ACAMS Today* about his vision for GIABA under his mandate and the current challenges in the regulatory environment.

ACAMS Today (AT): What led you to a career in anti-financial crime (AFC)?

Edwin W. Harris (EWH): I must first start by expressing my unqualified gratitude for providing me with a platform in *ACAMS Today*. My drive for taking a career shift into AFC stems from the inadequate provision of social services and economic injustices (in the sense of deprivation of basic social services due to public fraud, corruption, waste and abuse in public services) that permeate across our countries. Because of willful public corruption, the general public across our region has been denied many meaningful social services. If a public official steals, this automatically denies someone in the general public quality education, access to good health and food security. Hence, having a career that works toward preventing financial crimes and punishing those who betray public trust by carrying out these unwholesome practices remains my passion, which creates the space for bringing justice to the community for denying them basic social services.



AT: As the director general of GIABA, what would you like to accomplish during your tenure?

EWH: GIABA is mandated to protect West African countries' economies from financial crimes (i.e., money laundering, terrorist financing and other forms of financial crimes). It is against this backdrop that I am determined to protect our economies by creating the enabling environment for asset recovery with the establishment of an Economic Community of West African States (ECOWAS) sanctions regime, like the Office of Foreign Assets Control and the European Union. The logic of this sanctions regime is to escalate the preventive work done by GIABA to a level that we restrict assets, the movement of corrupt individuals, terrorist financiers and associates that continue to plague our region and undermine our collective security, peace and stability. The purpose behind this ECOWAS sanctions regime is to deter existing and would-be criminals by restricting their movement and confiscating illegal monies (proceeds of crimes). This level of deterrence will contribute a lot to protecting West African economies. In addition, I want to leave trained professionals in place that will have the skills and knowledge to take on the asset recovery campaign in Members States.

AT: Quite a few of your efforts have been focused on eradicating corruption in West Africa. Why has this been an important step in the AFC industry?

EWH: This effort is important because it is personal to me as an individual and affects the many children in the region who go to bed without food, do not have access to safe drinking water, have poor education and live with insecurity because of the state of corruption and unjust enrichment by the political elite and their associates. In addition, corruption has contributed to conflict and feud terrorism and has created an environment where our youth and nations cannot harness their potential to provide shared prosperity. The goal is to establish an inclusive environment where access to basic social services as a human being is a right and not a dream. It is important because it also adversely impacts our governance system. Corrupt individuals (the political elite and their associates) become richer and feel that the nation and its inhabitants are their possessions. Hence, fighting corruption, in my mind, also becomes a fight for basic human and fundamental rights where the needs and aspirations of all are guaranteed.

Another reason is to assist in working toward encouraging the public not to accept corruption as cultural socialization; it is a common practice in the region that those who engage in these financial crimes are celebrated in the community and praised for being good or philanthropic. In some instances, the community goes against AFC practitioners for naming corruption and shames them, and in other cases, the community undermines investigations because of connections to a politician or family member. When the community rejects corruption as part of our cultural socialization and sees it as the reason behind the lack of basic social services and the cause for instability in some countries, it

will provide an impetus to fight and create an environment that disincentivizes the practices of corruption and other financial crimes. These are some of the cardinal reasons why I am in AFC.

AT: What challenges lie ahead for the financial services sector in West Africa?

EWH: There are some challenges that are currently faced by financial services in the region, ranging from upgrading to current modern technologies, emergences of financial technology and the associated risks in financial crimes, regulatory demand and overall inflation in various countries that impact macroeconomics with an adverse effect on financial services. It must be noted that financial institutions (FIs) in the region are making some strides in curbing these challenges on several fronts. Also, the challenges in compliance culture in some segments within the financial services sector are gradually being addressed, which will grant greater compliance to regulatory obligations than before. FIs are filing suspicious transaction reports and currency transaction reports. However, designated nonfinancial businesses or professions still remain a challenge and an area of concentration because of the risk of unlawful activities, including money laundering and other forms of financial crimes.

Professional development should remain a focus for effectiveness

AT: How can AFC professionals be more effective in preventing financial crime?

EWH: First and foremost, AFC professionals should first be accepted and seen as individuals with high integrity whose character is undisputed. That is the first line of reputational defense that remains indispensable. Professionals should desire new skills and understand trends and methods as they evolve in the field. Professional development should remain a focus for effectiveness. In addition, sharing information and keeping the sanctity of your sources of information gathered remains cardinal to running an effective preventive measure. Deterrence should be used as a major tool for preventive methods. Where there is no deterrence, it is likely that crimes will continue to exist. Lastly, the legal framework should also be tailored to include preventive measures and not only punitive measures.

AT: What advice or recommendation would you like to share with AFC professionals?

EWH: My advice to AFC professionals is to be courageous, strong and determined to pursue their goals within the legal framework. AFC professionals should understand the difference between morality and legality. These are two keywords that sometimes compromise our work and, in some instances, allow us to become sentimental and emotional. In other words, we must remove emotions and sentiments from the work we do. It is in the best interest of AFC professionals to always remain ahead of the curve through professional development. AFC professionals should always endeavor to develop new skills and knowledge. Lastly, they should learn to network/share information and remain confidential. **AT**

Interviewed by: ACAMS Today editorial, ACAMS, editor@acams.org

Defining 'digital asset-related business'

What is a digital asset-related business (DARB)? All financial institutions (FIs) must have a clear answer to this question and take a vested interest in this complex asset class to effectively manage risk and monetize the opportunity. Regardless of an institution's policy toward digital assets themselves¹ or the ecosystem of businesses surrounding digital assets, poorly constructed policies and procedures are a risk to any effective compliance program. Although regulated institutions are encouraged to "take a risk-based approach in assessing individual customer relationships, rather than declining to provide banking services to entire categories of customers without regard to the risks presented,"² many continue to take the simplistic "just say 'no'" or risky "do not ask, do not tell" approach toward this industry. As a result, these institutions (a) have a limited understanding of digital assets and DARBs; (b) have not clearly defined "digital asset-related business"; and (c) therefore have nonexistent, unclear or incomplete policies and procedures, which can lead to inconsistent interpretation and implementation.

Leveraging prior work experience—which defines terminologies and taxonomies in the cannabis industry³ and recent discussions with top-tier FIs—this article shares a comprehensive and cohesive framework for defining DARBs and classifies them into three relevant risk-based tiers. FIs, regulators and policymakers will benefit from this framework when developing, revising or updating their digital asset-related policies and procedures.

Why is this relevant?

In March 2022, U.S. President Joseph Biden issued his "Executive Order on Ensuring Responsible Development of Digital Assets," which stated, "Advances in digital and distributed ledger technology for financial services have led to dramatic growth in markets for digital assets, with profound implications for the protection of consumers, investors, and businesses, including data privacy and security; financial stability and systemic risk; crime; national security; the ability to exercise human rights; financial inclusion and equity; and energy demand and climate change. In November 2021, non-state issued digital assets reached a combined market capitalization of \$3 trillion, up from approximately \$14 billion in early November 2016."⁴

More recently, in January 2023, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency (OCC) issued the "Joint Statement on Crypto-Asset Risks to Banking Organizations," which stated, "The events of the past year have been marked by significant volatility and the exposure of vulnerabilities in the crypto-asset sector..." and goes on to list a number of key risks to banking organizations.⁵

As such, national and international government agencies have been offering descriptions and definitions of digital asset-related businesses and have drafted regulations and guidelines to mitigate risk to FIs, investors and consumers. The Federal Reserve has stated that given the "heightened and novel risks" posed by digital assets, it is "closely monitoring banking organizations' participation" in digital asset-related activities.⁶ In April 2022, the OCC issued a consent order against "the first crypto-native bank,"⁷ noting the importance of anti-money laundering (AML)/Bank Secrecy Act elements in "novel digital asset activities."⁸ The OCC noted that prior to engaging in any digital asset-related activities—knowingly or unknowingly—FIs "must ensure such activity is legally permissible" and "have in place adequate systems, risk management, and controls to conduct such activities in a safe and sound manner and consistent with all applicable laws..."⁹

However, in order to effectively meet these guidelines, FIs need to clearly define DARBs and then develop risk-based policies and procedures specific to DARBs, including effective methods for consistently identifying, categorizing by risk-rating and treating accordingly.

A three-tiered risk approach

The following framework can be used to consistently define, identify and classify DARBs into three risk-based tiers, which effectively describe the degree to which a business "touches" digital assets and/or interacts with other DARBs. This multi-tiered approach can help FIs—including those that believe they have minimal exposure to the industry—to determine which businesses operating in the digital asset ecosystem they may be willing to offer products and services to and, equally important, to what extent they may need to update policies, procedures and due diligence methods to identify, measure and mitigate digital asset-related risk.

Most countries and states are still contemplating how to regulate DARBs, including which types/tiers of DARBs should be regulated and by whom

Tier 1A DARBs

Tier 1A DARBs are considered the riskiest because they directly “touch” digital assets and, as such, are the most likely to be licensed, regulated and supervised for AML and counter-terrorist financing purposes. Tier 1A also includes intermediaries “whose activities may increase risks to financial stability.” Domestically, the U.S. Securities and Exchange Commission (SEC) describes these intermediaries as those who are “involved with digital asset investment, trading, and safekeeping,”¹⁰ while internationally, the Financial Action Task Force (FATF) refers to them as virtual asset service providers (VASPs)¹¹ and Markets in Crypto-Assets (MiCA) refers to them as crypto-asset service providers (CASPs).¹² Tier 1A DARBs include, but are not limited to:

- Issuers
- Miners
- Exchanges and trading platforms¹³
- Order-taking and execution
- Custody and administration
- Wallets and ATMs

Tier 1B DARBs

A Tier 1B DARB is a business that either (a) invests directly in digital assets and/or (b) wholly owns, manages and/or controls one or more Tier 1A DARBs. This Tier 1B concept generally aligns with the SEC, which highlights digital asset exchange-traded funds, and CipherTrace, which highlights digital asset hedge funds.¹⁴ Segmenting between Tier 1A “operators” and Tier 1B “owner/investors” is helpful and warranted, even though they are in the same risk tier.

Tier 2 and Tier 3 DARBs

There are thousands of “indirect” or “ancillary” businesses that interact with Tier 1 DARBs but that do not “touch” digital assets and are not expected to be licensed/regulated. Generally, this class of DARBs is excluded from the concepts of FATF’s VASP and MiCA’s CASP, even though they still pose a high risk of possibly “aiding and abetting” any illicit digital asset activities that they support at their Tier 1 DARB clientele. For this reason, our framework contemplates and defines these as Tier 2 and Tier 3 DARBs.


Tier 2 DARBs are newer, smaller companies generally created specifically to participate in the digital asset economy focused on selling products and services to Tier 1s and generating “substantial” revenue (e.g., greater than 50%) from Tier 1s. A Tier 2 DARB would appear to align with what CipherTrace calls a “Digital Asset Entity,” which includes “gambling sites, incubators, and other entities which use [digital assets] but are not classed as financial institutions.”¹⁵ Examples of Tier 2 DARBs include, but are not limited to:

- Hardware manufacturers
- Software providers
- Fintechs
- Blockchain developers
- Pre-acquisition special purpose acquisition companies (SPACs)
- Professional services
- Energy providers

A note about regulation and licensing

Most countries and states are still contemplating how to regulate DARBs, including which types/tiers of DARBs should be regulated and by whom. As such, there are not any clear frameworks for licensing and regulating Tier 1 DARBs, even though Tier 1 DARBs clearly exist and operate. For this reason, whether a particular business is yet duly "licensed" by a national or state regulator is not directly relevant when determining if that business is a DARB.

Conclusion

The goal of this article is not to influence an FI's decision of whether to participate in digital asset-related businesses as an asset class but rather to share a framework for developing comprehensive policies and procedures to consistently and effectively make risk-based decisions regarding DARBs. 

Steven Kemmerling, founder and CEO, CRB Monitor, steve@crbmonitor.com

Jim Francis, CFA, head of research, CRB Monitor, james.francis@crbmonitor.com

The information provided in this article is not intended to be and should not be considered advice or authoritative guidance regarding any aspect of FI compliance with state, federal or international laws. CRB Monitor takes no responsibility and shall have no liability for the accuracy or completeness of the information contained in this article. FIs should consult with their compliance and legal departments regarding any of the information and any interpretations of such information as it may relate to the institution's facts and circumstances and their implementation of compliance procedures.

¹ CRB Monitor utilizes the term "digital asset" to align with the Biden Administration's, the SEC's and the Congressional Research Service's (CRS) usage. Per the SEC, "The term 'digital asset'... refers to an asset that is issued and transferred using distributed ledger or blockchain technology, including, but not limited to, so-called 'virtual currencies,' 'coins,' and 'tokens.'" Per the CRS, "Digital assets" are assets issued and transferred using distributed ledger or blockchain technology. They are often referred to as crypto assets,

cryptocurrency, or digital tokens, among other terminology." For further information, see "Digital Assets and SEC Regulation," *Congressional Research Service*, June 23, 2021, <https://crsreports.congress.gov/product/pdf/R/R46208>; "Framework for 'Investment Contract' Analysis of Digital Assets," *U.S. Securities and Exchange Commission*, April 3, 2019, <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>

² "FDIC Encourages Institutions to Consider Customer Relationships on a Case-by-Case Basis," *Federal Deposit Insurance Corporation*, January 28, 2015, <https://www.fdic.gov/news/news/press/2015/pr15009.html>

³ "Defining Marijuana Related Businesses," *ACAMS Today*, September–November 2016, Vol. 15 No. 4, <https://www.acamstoday.org/defining-marijuana-related-businesses/>

⁴ President Joseph Biden, "Executive Order on Ensuring Responsible Development of Digital Assets," *The White House*, March 9, 2022, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets>

⁵ "Joint Statement on Crypto-Asset Risks to Banking Organizations," *Federal Reserve, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency*, January 3, 2023 <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230103a1.pdf>

⁶ "Supervisory Letter SR 22-6 / CA 22-6 on engagement in crypto-asset-related activities by Federal Reserve-supervised banking organizations," *Federal Reserve*, August 16, 2022, <https://www.federalreserve.gov/supervisionreg/srletters/SR2206.pdf>

⁷ Anchorage Digital, <https://www.anchorage.com/>

⁸ "OCC Notes Importance Of BSA/AML Elements In Novel Digital Asset Activities," *National Law Review*, April 28, 2022, <https://www.natlawreview.com/article/occ-notes-importance-bsaaml-elements-novel-digital-asset-activities>

⁹ *Ibid.*

¹⁰ "Digital Assets and SEC Regulation," *Congressional Research Service*, June 23, 2021, <https://crsreports.congress.gov/product/pdf/R/R46208>

¹¹ "Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers," *Financial Action Task Force*, October 2021, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

¹² "MiCA (Updated July 2022): A Guide to the EU's Proposed Markets in Crypto-Assets Regulation," *Sygnia*, July 2022, <https://www.sygnia.io/blog/what-is-mica-markets-in-crypto-assets-eu-regulation-guide/>

¹³ For a summary of the differences between "exchanges" and "trading platforms," see "Is There a Difference Between Exchange and Trade Platform," *Medium.com*, October 23, 2018, <https://medium.com/@exlamadotcom/is-there-a-difference-between-exchange-and-trade-platform-493630522a7e>

¹⁴ "What is a Virtual Asset Service Provider (VASP)?" *CipherTrace*, <https://ciphertrace.com/glossary/virtual-asset-service-provider-vasp/>

¹⁵ "Digital Asset Entity," *CipherTrace*, <https://ciphertrace.com/glossary/digital-asset-entity/>

Tier 3 DARBs

Tier 3 DARBs are considered the least risky tier and not a "digital asset-related business" in the strictest sense. Like Tier 2s, Tier 3 DARBs are known to have Tier 1 DARBs as customers. However, unlike Tier 2s, Tier 3s are older, larger companies that historically operated outside of the digital asset economy that are not focused on selling products and services to Tier 1s and generate "unsubstantial" revenue (e.g., less than 50%) from Tier 1s. Fundamentally, Tier 3s differentiate from Tier 2s by age, focus and revenue concentration.

Wiggle room

This framework is meant to be flexible and allow for wiggle room so that each FI can adjust it as needed to "take a risk-based approach in assessing individual customer relationships." A few examples might include the following:

- **Increase risk tier:** Although professional services firms known to serve Tier 1 DARBs might be categorized as Tier 3 by default (the lowest risk and "limited risk"), if a large, mature firm develops a focus on digital assets and generates substantial revenue to come from the industry, it could reasonably be categorized as Tier 2.
- **Decrease risk tier:** Although digital asset custody businesses are categorized as Tier 1 by default (the highest risk and possibly "off-limits"), if a large, mature custodian bank begins to provide some digital asset custody services, one expects only incidental revenue from the new line of business; it could reasonably be categorized as Tier 2 or even Tier 3.
- **Add a new risk tier:** In lieu of using this simple three-tiered framework, in which Tier 2 and Tier 3 are differentiated by a single revenue-concentration limit, your institution might consider additional tiers/buckets to account for a sliding scale of revenue to allow for more granularity.





Eyeing compliance blind spots in bank-fintech partnerships

The digitization of banking is inevitable, and consumers are demanding it. PwC reported that direct (digital) banks' share of consumers' primary banking relationships rose by 80% from 2019 to 2021.¹ Traditional banks have long seen the writing on the wall regarding sinking customer satisfaction. A 2022 Gallup Poll revealed that trust in banking fell six percentage points from the previous year to 27%.² Customer satisfaction scores for retail banks are lowest in the category of helping their customers save time or money—which not only is a top priority for customers but also the disruptive value proposition of fintechs.³

Legacy retail banks do not have the resources nor expertise to launch the types of mobile, connected, 24/7 functionality that fintechs offer. At the same time, these smaller, tech-savvy firms lack the big budgets, built-out customer bases and market reputations that traditional banks have earned over decades. Banks are bringing fintechs into the fold to the trendy hybrid model by engaging in partnerships that range from banking-as-a-service providers, embedded relationships and white-label partnerships, in which a bank acquires the fintech or outsources services to a fintech. These new intermingling relationships between two disparate business models of technology and banking will align the financial system better with customer expectations. However, regulators, lawmakers, industry leaders and compliance leaders need to work together to understand the rapidly evolving system to prevent risk management blind spots from becoming reputational, security or operational crises down the road.

Conscious coupling: Fintechs and banks

Most are familiar with how Zelle's solution has been embedded with numerous bank platforms to provide payment tools. In October, the nation's oldest bank, BNY Mellon, announced partnerships with two tech providers to hold crypto for its customers and to meet the diligence and compliance needs of those customers.⁴ Meanwhile, Citibank engaged with fintech IntraFi in the spring to provide an automated mechanism for corporate and institutional clients to diversify their deposits across multiple institutions. Other banks use fintechs to provide customer interface and experience technology; money management and wealth management services; expedited credit underwriting and loan origination processes; as well as data breach and identity protection tools. While fintechs are pushing traditional banks to innovate, they are also providing new avenues for banks to differentiate themselves from others by offering specialized solutions like instant payments, buy-now-pay-later or online notarization. A perhaps unanswerable question surrounds whether integrating fintechs into the traditional banking ecosystem will help rebuild consumer trust or further erode it.

The (r)evolutionary steps of a new banking system

The partnerships between banks and fintechs are growing at an exponential rate, with nearly two-thirds of banks entering into at least one fintech partnership over the past three years.⁵ Banks averaged 2.5 fintech partners in 2021, and that number is growing, making a complex situation even more elaborate.⁶ These new collaborative relationships, along with the efforts to mainstream decentralized finance (DeFi) and cryptocurrency, are causing tectonic changes to the financial system, bringing with it greater cybersecurity, business and regulatory complexity. Compliance teams must get accustomed to recalibrating their sights toward moving targets to stay in position to mitigate reputational, regulatory and operational risk factors that emerge from the coupling of disruptor fintechs and risk-averse brick-and-mortar banks. The retail bank is not absolved from any compliance issues that originate from the fintech partner. Bank compliance teams should scrutinize potential fintech partners' diligence and compliance processes before acquiring or integrating them. Banks should investigate whether the fintech has things like solid consumer data protection practices and unbiased loan processes and whether it has robust measures to prevent money laundering or other crimes.

New models plus new risks equal new compliance challenges

As stated in September's release of the White House's first-ever Comprehensive Framework for Responsible Development of Digital Assets, the U.S. has been explicit about preserving an environment conducive to "advancing responsible innovation," including considering agency recommendations to create a federal framework to regulate nonbank payment providers.⁷ While fintechs are currently subject to regulatory standards at the state and federal levels, fintechs tend to take on more risk with their consumer lending, a securities portfolio and higher liquidity.⁸ Furthermore, fintechs' overall resilience has not been tested by a significant economic downturn. Banking compliance officers must consider these factors along with the consumer data privacy standards and the requisite governance, internal controls, cybersecurity controls, change management issues and IT operational resilience factors. All of which is to say that the growing integration of fintechs into the mainstream banking space makes it much more challenging to shine a light on risk and compliance blind spots. Legislative and regulatory bodies like the Financial Industry Regulatory Authority, the Financial Crimes Enforcement Network and the Office of the Comptroller of the Currency (OCC) are racing to understand the intricacies of these arrangements and appraise consumer safety as well as the macroeconomic risk factors.



Compliance teams venture into uncharted territory

The methods with which retail banks can leverage fintechs as a competitive advantage are limited only by their creativity—and capability for adaptive compliance. Compliance and risk managers at banks that partner with fintechs should make themselves experts on the risks emerging from these new working relationships, which lack transparency and regulatory clarity. They must also grapple with reconciling two different business models. The lines between Federal Deposit Insurance Corporation-backed, regulated banks and less-regulated upstart fintechs are blurring. The OCC's oversight strategies spring from the central tenet of preserving trust in our banking system. Trust is built on ensuring that new partnerships promote good customer experiences, consumer data privacy and healthy competition. The OCC is moving in a direction to identify and remove any potential blind spots in new and under-the-radar risks that this evolving system may produce. Compliance leaders should do likewise while also keeping their fingers on the pulse of the regulators' movements and intentions.

Regulatory bodies shine a light on fintech-bank arrangements

Recently, the OCC called on Blue Ridge Bank to improve the oversight of its fintech partners, resulting in the bank increasing its risk assessment, monitoring and response to compliance as well as anti-money laundering and the Bank Secrecy Act, just to name a few.⁹ In addition, the OCC and other government bodies are certainly going to propose new regulatory guardrails. For example, the existing fair lending law, the Community Reinvestment Act, may be compelled to increase the assessment level banks face and may limit how and when banks partner with fintech companies. In April 2022, the Consumer Financial Protection Bureau invoked its corresponding authority to supervise nonbank entities whose activities are thought to pose a

financial risk to consumers under the Dodd-Frank Act. The OCC is exploring the possibility of special-purpose national bank charters for fintech companies.¹⁰ As stated by the OCC's Acting Comptroller of the Currency Michael Hsu, "While crypto has grabbed the headlines for most of the past year, I believe fintechs and big techs are having a large impact and warrant much more of our attention."¹¹

Compliance leaders must mind the gaps

Compliance leaders should proactively seek answers for the very questions the OCC will be asking, such as who is responsible for what when things break; how resilient are banking services to stress at fintechs; how do banks prevent their customers from becoming the product and how are consumer protections maintained; how are bank and fintech business models changing; and how are incompatibilities reconciled? The OCC is working on a process to subdivide bank-fintech arrangements into cohorts with safety and soundness risk profiles and attributes. But it is not always the known risks that can bring you down; it is the ones you might not predict. Fintechs that want to partner with banks should consider proactively reviewing their existing risk management and consumer compliance management program; assessing the program's processes and controls for potential gaps; and testing existing controls' design and operating effectiveness.

Most legacy banks will need to modernize and upgrade their legacy compliance and technology infrastructures that are slow and costly to adapt. Moving forward, banks and fintech partners should bake compliance requirements into the fabric of product development and customer engagement while remaining user-friendly. Compliance officers at banks that partner with fintechs have herculean tasks ahead of them and

should look at ways to automate processes, including compliance monitoring, reporting and regulatory intelligence, or at least ensure appropriate disclosures and other materials are inventoried in the right place. Undoubtedly, the costs of fortifying compliance teams, technologies and procedures will increase for banks partnering with fintech companies. However, the cost is well-balanced by high-stakes peace of mind, and, as banking leaders know, robust compliance aims not only to avoid penalties but also to achieve better business outcomes.

Preventing compliance blind spots from becoming compliance crises

If bank compliance teams can work well with their fintech partners to stay ahead of evolving regulations while also being vigilant in appraising and mitigating risks, they can successfully prevent compliance blind spots from becoming compliance crises. The OCC's Michael Hsu cautioned that if we do not map out and mitigate the risks generated from this trend toward bank-fintech arrangements, then we could see a crisis, not unlike the economic crisis of 2008, when the "failure to understand dynamics between traditional and shadow banking created a massive blind spot for the industry and regulatory community."¹² The International Monetary Fund, in its 2022 Global Financial Stability Report, warns "the combination of fast growth and the increasing importance of fintech financial services for the functioning of financial intermediation gives rise to systemic risks."¹³ The U.S. is heeding these alarm bells as it is innovating its oversight of banking, sincerely determined to instill trust within the system while allowing innovations to flourish. **AT**

Ben Richmond, founder and CEO, CUBE

- ¹ "PwC's 2021 Digital Banking Consumer Survey," *PwC*, <https://www.pwc.com/us/en/industries/financial-services/library/digital-banking-consumer-survey.html>
- ² Jeffrey M. Jones, "Confidence in U.S. Institutions Down; Average at New Low," *Gallup*, July 5, 2022, <https://news.gallup.com/poll/394283/confidence-institutions-down-average-new-low.aspx>
- ³ "U.S. Retail Banks Struggle to Differentiate, Deliver Meaningful Customer Experience as Economy Sours, J.D. Power Finds," *J.D. Power*, April 7, 2022, <https://www.jdpower.com/business/press-releases/2022-us-retail-banking-satisfaction-study>
- ⁴ Stacy Elliot, "BNY Mellon Launches Bitcoin, Ethereum Custody Services for Investment Firms," *Decrypt*, October 11, 2022, <https://decrypt.co/111641/bny-mellon-launches-bitcoin-ethereum-custody-services-investment-firms>
- ⁵ "The state of the union in Bank-FinTech partnerships," *Synctera*, <https://www.synctera.com/post/the-state-of-the-union-in-bank-fintech-partnerships#:~:text=Nearly%20two%2Dthirds%20of%20banks,in%20a%20FinTech%20in%202022>
- ⁶ "Average number of fintech and bank partnerships in the United States from 2019 to 2021," *Statista*, <https://www.statista.com/statistics/1315142/us-number-of-bank-fintech-partnerships/>
- ⁷ "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets," *The White House*, September 16, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/>
- ⁸ Antonio Garcia Pascual and Fabio Natalucci, "Fast-Moving FinTech Poses Challenge for Regulators," *IMF Blog*, April 13, 2022, <https://www.imf.org/en/Blogs/Articles/2022/04/13/blog041322-sm2022-gfscr-ch3>
- ⁹ "OCC Enforcement Actions and Terminations," *Office of the Comptroller of the Currency*, October 20, 2022, <https://occ.gov/news-issuances/news-releases/2022/nr-occ-2022-130.html>
- ¹⁰ "Exploring Special Purpose National Bank Charters for Fintech Companies," *Office of the Comptroller of the Currency*, December 2016, <https://www.occ.gov/topics/supervision-and-examination/responsible-innovation/comments/pub-special-purpose-nat-bank-charters-fintech.pdf>
- ¹¹ "Acting Comptroller of the Currency Michael J. Hsu Remarks at the TCH + BPI Annual Conference 'Safeguarding Trust in Banking: An Update,'" *Office of the Comptroller of the Currency*, September 7, 2022, <https://www.occ.treas.gov/news-issuances/speeches/2022/pub-speech-2022-106.pdf>
- ¹² *Ibid.*
- ¹³ "The Rapid Growth of Fintech: Vulnerabilities and Challenges For Financial Stability," *IMF*, April 2022, <https://www.imf.org/-/media/Files/Publications/GFSR/2022/April/English/ch3.ashx>



Over the past decade and a half, some of Russia's wealthiest and most powerful people, with the blessing of President Vladimir Putin, have been working on boosting Russia's soft power in the world of sports. The Russian Kontinental Hockey League (KHL) was to become the dominant ice hockey league in all of Eurasia, possibly equivalent to the National Hockey League (NHL), the North American ice hockey league, considered the best in the world. Russia's recent behavior, however, provoked a strong and united international response that, among other sectors, had a profound impact on Russian ice hockey.

The historical significance of ice hockey in Russia

In Russia, ice hockey has a long tradition. Russian hockey is internationally recognized for its glorious past—the Soviet Union's men's national ice hockey team, the "Red Machine," which dominated world hockey between 1950 and 1980, winning seven Olympic gold medals and acquiring an enormous symbolic significance for the Soviet regime. To this day, Russia still has a top national hockey team, currently ranked third in the world by the International Ice Hockey Federation.¹ According to recent estimates, the country has more than 110,000 registered players. Only the Czech Republic, Canada and the U.S. boast larger pools of players.²

Due to its historical significance for the country, ice hockey enjoys particularly strong support from the highest echelons of Russia's power hierarchy. President Putin is an active player, regularly participating in gala matches alongside other members of Russia's elite. It has even been reported that hockey is the most popular sport among senior officials and businessmen in Russia. Taking part in those games is seen as a symbol of closeness to the Russian president.³

But Putin's professed love for the game does not end with his participation in all-stars gala exhibitions where he regularly scores half of his team's goals. He

has also been personally involved in the development of the Russian hockey league. In 2011, a Russian online sports outlet quoted Putin as saying that the ice hockey world suffered since the end of the confrontation between North American and Soviet hockey. He said that after the dissolution of the Soviet Union, the NHL became "a vacuum cleaner" for all of the world's ice hockey talent.⁴

With the stated goal of "furthering the development of hockey throughout Russia and other nations across Europe and Asia," the KHL was founded in March 2008.⁵ Putin was quoted by the Russian media as saying that he not only fully supported the KHL, but that he was the league's main initiator. His stated goal was that KHL would turn into an All-European hockey league, expanding beyond Russia's borders to traditional European hockey powerhouses, such as Sweden, the Czech Republic and Switzerland.⁶

The Russian president mobilized the required funding for the league from a group of loyal oligarchs and key corporate sponsors such as Gazprom or Rosneft.⁷ People from Putin's closest inner circle were installed in the top positions of Russian hockey.

Russian ice hockey in trusted hands

The role that ice hockey plays in Russian politics and business has been compared to golf in the U.S. Especially since Putin found his passion for the game, hockey has reportedly become the most popular sport among senior officials and businessmen in Russia. Important Russian political figures, such as Defense Minister Sergei Shoigu, Prime Minister Mikhail Mishustin or Putin's former chief security guard and current Governor of Tula Region Aleksey Dyumin, regularly appear on the ice with the Russian president.⁸

The very top positions in Russian hockey are reserved for those who have proven their loyalty to the Russian president. This

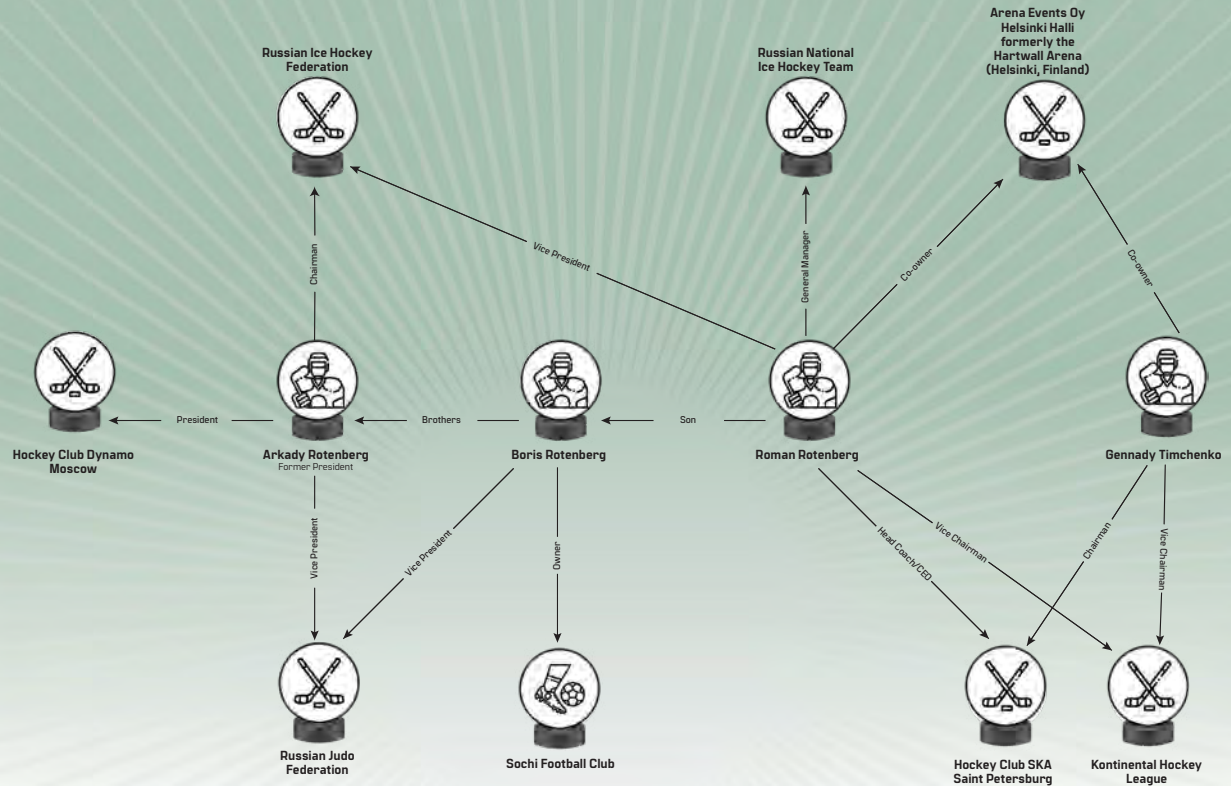
applies perhaps to no one more than to the Rotenberg family. The brothers Boris and Arkady Rotenberg are both Putin's childhood friends and judo partners from his Saint Petersburg days. The two brothers, along with Boris's son Roman Rotenberg and Gennady Timchenko, another Kremlin insider who has been described as Putin's "number one banker," hold the most powerful positions in Russian ice hockey.⁹

As shown in Graphic 1, the older brother Arkady Rotenberg currently serves as the chairman of the Russian Ice Hockey Federation, the governing body overseeing ice hockey in Russia, and the president of HC Dynamo Moscow, one of the most successful ice hockey clubs in Russia. Beyond ice hockey, Arkady Rotenberg also serves as the first vice president of the Russian Judo Federation.

His younger brother Boris owns both major sports clubs in the Russian city of Sochi: The Sochi Football Club and Hockey Club Sochi. He also serves as vice president of the Russian Judo Federation. Perhaps even more interesting is the career trajectory of Boris' son Roman Rotenberg who currently serves as general manager of the Russian National Ice Hockey Team and vice president of Hockey Club SKA Saint Petersburg, a dominant force in the KHL.

However, this did not seem to be enough for the ambitious young oligarch. In January 2022, Roman Rotenberg, who has never served as a coach or played the game professionally, was named the head coach of SKA Saint Petersburg. In this context, it is important to add that the club is owned by the Russian state-controlled energy company Gazprom and presided over by Timchenko, a close ally of both Putin and the Rotenberg family. Notably, Timchenko has also been the chairman of the KHL itself since 2012.¹⁰

Graphic 1: Rotenberg family breakdown



Visualization by Filip Brokes

KHL’s international expansion

Putin’s close ally Timchenko was entrusted with an ambitious project—to transform the domestic Russian hockey league into a vast Pan-Eurasian hockey league with prestige and resources on par with the North American NHL.

The initial plans foresaw the creation of a Pan-European championship of 64 club teams divided into Scandinavian and Central European sub-conferences.¹¹ The first non-Russian teams to join the league were Dinamo Riga from Latvia, Dinamo Minsk from Belarus and Barys Astana from Kazakhstan. All three of those clubs participated in the first season of 2008/2009.

The first expansion beyond the borders of the former Soviet Union was realized in 2011 when the Slovakia-based Lev Poprad (later renamed and relocated Lev Praha) joined the league. In 2013, Lev Poprad was followed by the Croatia-based Medvescak Zagreb, and in 2014, the first Scandinavian team joined the league, the top Finnish team Jokerit from Helsinki.

At that point, the Russian KHL started to attract international players from top ice hockey nations, such as Canada, the U.S., Sweden, Finland and the Czech Republic. Only a few years after its creation, the KHL was already considered the second-best ice hockey league in the world, with the NHL still being regarded as the best league.¹²

However, in 2014, the expansion stalled and negotiations with Swedish, German, Swiss, Austrian and other European teams that were conducted mostly in the early 2010s did not bear any results.¹³

Undoubtedly, Russia’s annexation of the Crimean Peninsula from Ukraine in early 2014, and the subsequent deterioration of relations between Russia and the West did not help to increase the KHL’s attractiveness. The still interested European-based teams suddenly faced potentially serious reputational issues attached to joining the Russian ice hockey league.

Furthermore, in March 2014, the U.S. imposed sanctions on 20 Russian individuals believed to be part of Putin’s inner circle. The list included both the Rotenberg brothers and



Alexander Lukashenko (left), president of Belarus, talks with Russian tycoon Gennady Timchenko during an ice hockey game in Sochi, Russia, in February 2019. Photo by Sergei Chirikov/Pool via *Reuters*

Gennady Timchenko, key decision-makers in Russian ice hockey.¹⁴ This was a heavy blow to Russia's ice hockey expansionist agenda.

Nevertheless, the first round of sanctions did not seem to have a major impact on the league. Far more consequential for Russian ice hockey were the events following the Russian invasion of Ukraine.

The aftermath of the Russian invasion of Ukraine

Almost immediately after Russia invaded Ukraine in February 2022, the Helsinki-based KHL team Jokerit withdrew from the league playoffs to protest the invasion. The Finnish team was soon followed by the other European-based KHL team, the Latvian Dynamo Riga, whose leadership also decided to withdraw the team from the KHL.¹⁵

Also, in response to the invasion, the International Ice Hockey Federation (IIHF) suspended all Russian and Belarusian national teams and clubs from participation in every age category and all IIHF competitions, including the world championship.¹⁶

Similarly, the NHL suspended the operation of their Memorandum of Understanding with the Russian KHL, officially severing communication between the two leagues. The NHL also instructed the league teams to "immediately cease all dealings with the KHL and KHL clubs, as well as with player agents who are based in Russia."¹⁷

Moreover, immediately after the invasion, the U.K. imposed sanctions on five Russian banks and three oligarchs. Notably, the three sanctioned oligarchs were Gennady Timchenko, Boris Rotenberg and Igor Rotenberg. Under the sanctions, all of their U.K. assets are frozen and dealing with U.K. individuals and entities, as well as access to the U.K., is denied.¹⁸

Similarly, the U.S. re-imposed sanctions on the Rotenberg brothers, this time including Boris' son Roman, cutting them off from the U.S. financial system, freezing their U.S.-based assets and blocking their property from use.¹⁹

More significantly for Russian ice hockey, the European Union (EU) imposed sanctions on Timchenko and both of the Rotenberg brothers, which has had a profound impact on their ice hockey-related assets in Finland.



In January 2022, Roman Rotenberg (left), son of President Vladimir Putin's childhood friend Boris Rotenberg, was named the head coach of SKA Saint Petersburg, despite never having served as an ice hockey coach or having played the game professionally. Photo by Global Look Ltd.

Top Finnish ice hockey club in Russian hands

The Helsinki-based ice hockey club Jokerit joining the Russian KHL was a direct consequence of the preceding inflow of Russian capital into Finnish ice hockey. In the summer of 2013, Timchenko and the Rotenberg brothers acquired a minority stake in Jokerit (49%) and also a stake in the club's home rink and Helsinki's largest stadium, the Hartwall Arena (44.89%).²⁰

Only a year later, after international sanctions were imposed on the three individuals, Arkady and Boris Rotenberg sold their shares in both the club and the stadium to the latter's 33-year-old son Roman Rotenberg. The transfer gave Roman Rotenberg a 50.5% stake in Arena Events, the company that owned the Finnish assets, with the rest being held by Timchenko.²¹

However, the club soon got into serious financial difficulties, reportedly losing more than 50 million euros (over \$53 million) during its first five seasons in the KHL. On top of that, financing the club was difficult due to the U.S. sanctions imposed on Timchenko. Reportedly, there were frequent delays in money transfers from Timchenko's to Jokerit's bank account. Players' salary payments were often delayed.

This issue was eventually resolved in the summer of 2019 when Timchenko and Rotenberg sold their stake in the Finnish club to the Nor Nickel group of the Russian oligarch Vladimir Potanin who at the time was not included on any sanctions list.²² However, the two kept their stake in the ice hockey arena.

Potanin was long able to escape sanctions due to his role in the production of important raw materials. However, after Russia invaded Ukraine, the oligarch was targeted by both Canada and the U.K. with personal sanctions.²³ Potanin then decided to sell his stake in Jokerit to the club's Finnish general manager Jari Kurri.²⁴

Nevertheless, even after the Russian invasion of Ukraine and Jokerit's subsequent withdrawal from the KHL, Roman Rotenberg and Gennady Timchenko still continued to hold stakes in the club's home arena. This was causing a heavy public backlash in Finland, with many of the arena's sponsors withdrawing their partnerships.

At this point, Timchenko was sanctioned by all major western countries, including the EU. Finland's National Enforcement Authority eventually took advantage of the EU sanctions and confiscated Timchenko's stake in the arena (22.5%). The same could not be done with Rotenberg's stake. Even though he has been sanctioned by the U.S., U.K., Canada and Switzerland, he has not appeared on the EU sanctions list, making the freezing of his Finnish assets impossible.²⁵

Conclusion

Under the current circumstances, Rotenberg and Timchenko have to ask the Finnish National Enforcement Authority for permission to sell their stakes in the arena. They would not receive any money from the sale until the Authority unseized the asset.²⁶ According to an article published by the Finnish daily *Helsingin Sanomat* in late 2022, the sale of the arena is currently ongoing. Furthermore, even though international sanctions make the deal complicated, several "serious buyers" have expressed interest in the "iconic arena."²⁷

The forced sale of both the Finnish club and its arena by the Russian "ice hockey oligarchy" is symbolic of the current state of ice hockey in the country. Russia is cut off from all international competitions. Key Russian ice hockey decision-makers are under international sanctions. Foreign players are leaving the KHL en masse, and the league itself has rolled back from Europe to Russia and Asia. By almost all measures, it seems that Putin's grand plan for an all-powerful, Moscow-centered, Eurasian ice hockey league has failed. With that, the competitiveness of Russian ice hockey on the international scene might suffer as well. It remains to be seen how competitive Russian ice hockey will be once it reenters the international stage, whenever it might be. **AT**

Filip Brokes, senior analyst, Berlin Risk Advisors GmbH, Berlin, Germany, filip.brokes@berlinrisk.com

¹ "World Ranking," *International Ice Hockey Federation*, <https://www.iihf.com/en/worldranking>

² "Countries ranked by number of registered ice hockey players in 2021/22," *Statista*, <https://www.statista.com/statistics/282349/number-of-registered-ice-hockey-by-country/>

³ Romain Colas, "He shoots, he scores! Putin's hockey passion shapes Russian elite," *Agence France-Presse*, January 22, 2020, <https://sports.yahoo.com/shoots-scores-putins-hockey-passion-shapes-russian-elite-115702749--nhl.html?>

⁴ Artem Zyryanov, "Vladimir Putin on hockey. 20 statements by the [President] of Russia," *Sports.ru*, November 19, 2011, <https://www.sports.ru/tribuna/blogs/centre/199850.html>

⁵ "About the KHL," *Kontinental Hockey League*, <https://en.khl.ru/official/about/>

⁶ Artem Zyryanov, "Vladimir Putin on hockey. 20 statements by the [President] of Russia," *Sports.ru*, November 19, 2011, <https://www.sports.ru/tribuna/blogs/centre/199850.html>

⁷ "Russia's Cultural Statecraft," *Routledge*, November 5, 2021, <https://www.routledge.com/Russias-Cultural-Statecraft/Forsberg-Makinen/p/book/9780367694357>

⁸ Romain Colas, "He shoots, he scores! Putin's hockey passion shapes Russian elite," *Agence France-Presse*, January 22, 2020, <https://sports.yahoo.com/shoots-scores-putins-hockey-passion-shapes-russian-elite-115702749--nhl.html?>

⁹ Vesa Rantanen, "Comment: Roman Rotenberg shocked you by becoming the head coach of the KHL's club—an even more outrageous background pattern extends directly to Putin," *Ilta Sanomat*, <https://www.is.fi/urheilu/art-2000008553103.html>

¹⁰ RFE/RL's Russian Service, "Son Of Putin Ally Lands Top KHL Post Despite No Ice Hockey Coaching Experience," *RadioFreeEurope RadioLiberty*, January 4, 2022, <https://www.rferl.org/a/putin-hockey-petersburg-rotenberg-coach/31639379.html>

¹¹ "Russia's Cultural Statecraft," *Routledge*, November 5, 2021, <https://www.routledge.com/Russias-Cultural-Statecraft/Forsberg-Makinen/p/book/9780367694357>

¹² Eugene Helfrick, "Top 10 Best Ice Hockey Leagues," *The Hockey Writers*, updated January 3, 2023, <https://thehockeywriters.com/top-10-best-ice-hockey-leagues/>

¹³ "Russia's Cultural Statecraft," *Routledge*, November 5, 2021, <https://www.routledge.com/Russias-Cultural-Statecraft/Forsberg-Makinen/p/book/9780367694357>

¹⁴ Tom Miles, "U.S. sanctions hit Gunvor co-founder, Rotenberg brothers," *Reuters*, March 20, 2014, <https://www.reuters.com/article/us-ukraine-crisis-sanctions-gunvor-idUSBREA2J1T920140320>

¹⁵ Diane Doyle, "Two Teams Pull Out of KHL to Protest Russian Invasion Of Ukraine," *NoVa Cap Fans*, February 27, 2022, <https://novacapsfans.com/2022/02/27/two-teams-pull-out-of-khl-to-protest-russian-invasion-of-ukraine/>

¹⁶ "IIHF Council takes definitive action over Russia, Belarus," *International Ice Hockey Federation*, February 28, 2022, https://www.iihf.com/en/news/32301/iihf_council_announces_decisions_over_russia_belar

¹⁷ Frank Seravalli, "Seravalli: NHL officially severs ties, communication with Russia's KHL," *Daily Faceoff*, March 7, 2022, <https://www.dailyfaceoff.com/seravalli-nhl-officially-severs-ties-communication-with-russias-khl/>

¹⁸ Sophie Morris and Greg Heffer, "Ukraine crisis: Five Russian banks and three oligarchs targeted in UK sanctions on Moscow—but MPs call for more action," *Sky News*, February 22, 2022, <https://news.sky.com/story/ukraine-crisis-five-russian-banks-and-three-high-net-worth-individuals-targeted-in-uk-sanctions-on-moscow-12548650>

¹⁹ "FACT SHEET: The United States Continues to Target Russian Oligarchs Enabling Putin's War of Choice," *The White House*, March 3, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/03/fact-sheet-the-united-states-continues-to-target-russian-oligarchs-enabling-putins-war-of-choice/>

²⁰ Kasper Viita, "Putin Allies Buy Finnish Hockey Team to Play for Russian Title," *Bloomberg*, June 28, 2013, <https://www.bloomberg.com/news/articles/2013-06-28/putin-allies-buy-finnish-hockey-team-to-play-for-russian-title?leadSource=uverify%20wall>

²¹ "Sanctioned Russian Billionaires Sell Finnish Hockey Team," *The Moscow Times*, October 10, 2014, <https://www.themoscowtimes.com/2014/10/10/sanctioned-russian-billionaires-sell-finnish-hockey-team-a40288>

²² Marko Lempinen and Arja Paananen, "This is how Jari Kurr's Jokerit is financed—in the background is a new Russian oligarch," *Ilta Sanomat*, June 7, 2019, <https://www.is.fi/khl/art-2000006134215.html>

²³ "Russia's richest man fights off Western sanctions," *The Brussels Times*, July 7, 2022, <https://www.brusselstimes.com/250747/russias-richest-man-fights-off-western-sanctions>

²⁴ "Jari Kurri takes full ownership of ex-KHL hockey club Jokerit," *YLE*, <https://yle.fi/a/3-12406995>

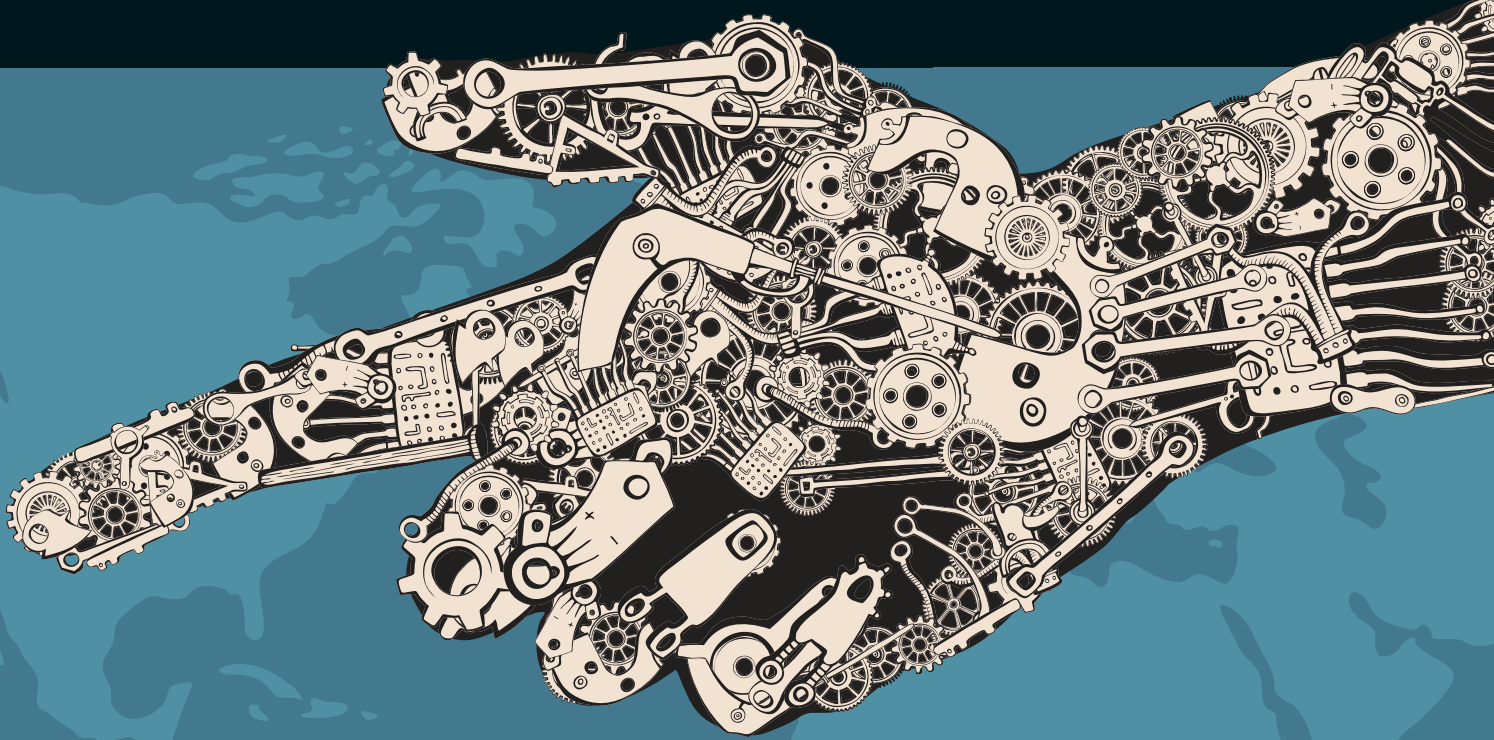
²⁵ "Russia Sanctions Database," *Atlantic Council*, <https://www.atlanticcouncil.org/blogs/econographics/russia-sanctions-database/>

²⁶ "Finland seizes Russian oligarch's Helsinki arena holdings," *YLE*, <https://yle.fi/news/3-12420021>

²⁷ Milla Paikoahto HS, Lari Malmberg HS and Valterri Parikka HS, "Russian oligarchs decided to sell their share: Helsinki Hall is going to be sold," *Helsingin Sanomat*, November 18, 2022, <https://www.hs.fi/kaupunki/art-2000009210299.html>



Faded glory: The vestiges of a removed neon sign mark the exterior of the former Hartwall Arena in Helsinki, Finland. Photo by Thor Kottelin



WHY TERRORIST ORGANIZATIONS use HUMAN TRAFFICKING



Editor's note: This article is the second part of a two-part series on human trafficking and terrorist organizations. The first part is available on ACAMSToday.org.¹

Human trafficking (HT) is used by terrorist organizations to exploit individuals and to carry out or support terrorist activities. In fact, terrorist organizations using HT for financial gain appear to be rarer than the trafficking of human beings for other exploitative purposes that support the organizations' activities. The Financial Action Task Force (FATF) highlighted that the small amounts generated by the Islamic State [group] in Iraq and the Levant (ISIL [IS throughout the article], also known as Da'esh) indicate that HT is not a lucrative source of revenue for IS and concluded that HT is considered more as a means of meeting the demands of IS fighters.² In this regard, the individuals who are held captive by terrorist organizations are mainly enslaved and forced into labor so fighters can devote their attention to their respective activities. The enslavement of individuals results in the free provision of services, which is not quantifiable in monetary terms but cuts operational costs and increases organizational efficiency.

SEXUAL EXPLOITATION

In a study conducted by the Henry Jackson Society, Nikita Malik stated, "Terrorists use sexual violence, including rape, sexual slavery, and forced marriage, to bolster recruits, galvanize fighters, and, in the case of Islamist groups, punish a Kafir (Arabic for disbeliever)."³

Women may also be sexually exploited for the purpose of forced impregnation. The Organization for Security and Co-operation in Europe (OSCE) reported a case involving 10 women between the ages of 19 and 38 from the South Caucasus region who were forcefully taken to Iraq by their husbands. When their husbands died, the women were forced to remarry, with nine of them delivering 45 children.⁴

LABOR EXPLOITATION

The Counter-Terrorism Committee Executive Directorate (CTED) stated that "men and boys have been not only forcibly recruited and indoctrinated but also subjected to forced labour in agriculture (e.g., on sheep and poultry farms in Iraq) and on construction projects. One example of the latter is [IS'] use of trafficked people to build a tunnel system under the streets of Mosul. The tunnels were responsible for significant casualties and for extending the siege of the city."⁵

Fighters can also benefit from individuals held in slavery in various ways, such as by "employing" them in their homes as domestic servants. For example, the United Nations Human Rights Council (UNHRC) reported, "Yazidi women and girls are forced to cook for their respective fighter-owners and other [IS] fighters housed with or near him. One Yazidi girl, 13 years old, was held for 11 months in [IS-controlled] territory and sold multiple times. Sexually enslaved, she recounted also being forced to cook, clean and wash the clothes of her Syrian fighter-owner and his family at a house in Raqqah city."⁶

THE ENSLAVEMENT OF INDIVIDUALS RESULTS IN THE FREE PROVISION OF SERVICES, WHICH IS NOT QUANTIFIABLE IN MONETARY TERMS BUT CUTS OPERATIONAL COSTS AND INCREASES ORGANIZATIONAL EFFICIENCY

HT AS A TERRORIST TACTIC

HT, in the context of terrorism, can be used by terrorist organizations to achieve some of their strategic objectives. CTED identifies three purposes for the strategic use of HT by terrorist organizations: Namely, to intimidate populations and decimate communities, to institutionalize sexual violence and slavery, and to drive recruitment efforts.

To intimidate populations and decimate communities

One of the most notable examples of the use of HT to intimidate populations and decimate communities is the IS's ethnic cleansing targeting minorities, especially the Yazidi community. Among these minorities, it is also worth mentioning the Shia Turkmen, Shia Shabak and Christian communities, which were considered "infidel unbelievers" and therefore persecuted. In addition to the severe violence perpetrated against these minorities, HT is used in its most horrendous form, where individuals are considered commodities. In this regard, IS engaged in the trade and purchase of unmarried women and girls in open slave markets, while boys were forcibly recruited and given new names, trained for combat in camps and used as human shields.⁷

To institutionalize sexual violence and slavery

The Report of the Secretary-General on Conflict-Related Sexual Violence published by the United Nations Security Council in 2018 stated that conflict-related sexual

violence is a weapon of war and a source of profit for state actors and non-state armed groups. In addition, the report pointed out, "Wars are still being fought on and over the bodies of women, to control their production and reproduction by force. Across regions, sexual violence has been perpetrated in public or witnessed by loved ones, to terrorize communities and fracture families through the violation of taboos, signifying that nothing is sacred and no one is safe."⁸ Acts of sexual violence, domestic servitude and other forms of sexual enslavement have been at the core of IS, Boko Haram and Al-Shabaab's modus operandi. For example, in the territory occupied by IS in Iraq, Sunni women and girls endured forced marriages as well as rape as a way of punishment for disobeying IS rules. In Nigeria, women and girls endured the same forms of sexual violence by Boko Haram members and faced acute social stigmatization upon their return because they were seen as sympathizers. In Somalia, there were reports of women and girls being trafficked by Al-Shabaab by being held as sex slaves or forced to become the "wives" of insurgents. Many of these women and their children were deeply traumatized and reluctant to seek assistance for fear of persecution.

To drive recruitment efforts

In addition to using HT to recruit individuals for various brutal purposes, such as sexual and labor exploitation, combat or service roles, terrorist organizations use these HT victims to attract new recruits. This strategy can be observed in IS propaganda campaigns, which aim to lure potential male fighters to join their cause. The sexual slavery propaganda serves as an incentive for new recruits and foreign fighters, with the promise of wives and sex slaves acting as a "pull factor."⁹ *The New York Times* has also reported, "The trafficking of women has been used to reward fighters, and as a recruiting tool to lure men from deeply conservative Muslim societies, where casual sex is taboo and dating is forbidden."¹⁰ In addition, children are often featured in IS propaganda through "[photographs] eulogizing them as martyrs and widely circulated videos of young boys executing (via shootings or beheadings) prisoners accused of being spies or captured Syrian regime troops."¹¹

HT AND TERRORIST FINANCING

As per the FATF, terrorist financing can be defined as the financing of terrorist acts, terrorists and terrorist organizations.¹² As previously mentioned, terrorist organizations using HT for financial gain seems to be rarer than the trafficking of human beings for other exploitative purposes to support the organizations' activities. This can be partly attributed to the fact that terrorist organizations operate primarily in conflict-stricken regions where access to formal financial services is

limited (e.g., the Sahel region in sub-Saharan Africa). In addition, as the FATF indicates, "The purposes and processes of terrorist financing and related activities are fundamentally different from those of money laundering; and 'money is only one of a number of essentially interchangeable instruments that can be exchanged for one another' in order for terrorist groups to obtain the end-use goods and other resources they need."¹³ These factors are based on the Terrorist Resourcing Model published by the Integrated Threat Assessment Centre (ITAC) in 2007, which stresses that terrorist entities do not depend only on money to power their operations. It is also worth highlighting that money laundering is based on greed, while terrorist financing/resourcing is primarily based on pushing a political or ideological agenda. In the context of terrorist financing/resourcing, money and other resources are the enablers of their activities.

Nevertheless, financial gain remains one of the reasons terrorist groups engage in the trafficking of human beings. The FATF stated that "terrorist organizations who have controlled, or partially controlled territory, have used human trafficking as a way to raise funds and support [for] their organizations and activities."¹⁴ It is also worth pointing out that unlike drugs, oil or other single-use goods, enslaved individuals are considered as "reusable commodities" as they can be exploited many times and for several purposes.

Enslaving women

In addition to gratifying their fighters, terrorist organizations enable individual fighters to generate revenue through the sale of women. FATF stated that "[IS] has provided internal guidance to its fighters regarding how many female slaves they are allowed to maintain; however, the prices [IS] fighters are paying for their slaves appear to be relatively low (approximately

\$13)."¹⁵ UNHRC reported that "Some Yazidi women and girls were present at their sale, and were aware of the amounts paid for them, which ranged between [\$200 and \$1,500], depending on marital status, age, number of children, and beauty."¹⁶ It is important to point out that slave markets are intended to be internal only. As a result, it is arguable whether the IS slave trade constitutes terrorist financing. In addition, the sale and resale sale of Yazidi women and girls outside of IS is forbidden and punishable by death because slaves are considered the spoils of war, as well as to prevent them from being sold back to their families, given that fighters would earn significant amounts ranging from \$10,000 to \$40,000. However, as CTED states, such rules are frequently violated.¹⁷

Trafficking in persons for ransom

Trafficking in persons for ransom is part of a terrorist organization's strategic objectives to fuel insecurity, and it also represents a highly profitable funding source. As a result, it is a common modus operandi for terrorist organizations. Unlike the sale of women, which is supposed to be internal only, the ransom payment constitutes terrorism financing since the payment is made by individuals outside the terrorist organization. While it is possible to argue whether ransom constitutes a form of exploitation,¹⁸ it is worth noting that individuals may be abducted for the purpose of ransom. In addition, in the context of terrorism, the ransom is the final element of the exploitation to which individuals are subjected. In this regard, terrorist organizations derive financial or other kinds of benefits from their exploitation, which amounts to HT.

CTED stated that "Many terrorist groups (notably [IS], Al-Nusra Front for the People of the Levant (ANF), Al-Qaida in the Arabian Peninsula (AQAP), Boko Haram and the Abu





WITHOUT HUMAN AND FINANCIAL RESOURCES, THE CAPABILITY AND ACTIVITY OF TERRORIST ORGANIZATIONS ARE DEGRADED

Sayyaf Group (ASG)) continue to profit from [kidnapping for ransom].¹⁹ According to CTED, the financial gain terrorist organizations derive from ransom is significant, as families would “pay between \$10,000 and \$40,000 to secure the release of their family members.”²⁰ In addition, the United Nations Security Council highlighted, “According to the United Nations Assistance Mission for Iraq (UNAMI), [IS] received between \$35 million to \$45 million in 2014 from ransom payments made by the families of hostages. It is believed that \$850,000 was paid in January 2015 for the release of 200 Iraqi Yazidi.”²¹ In addition, the BBC reported, “At least 1,409 students were kidnapped from their schools in northern Nigeria in the 19 months between March 2020 and September 2021, according to Nigerian intelligence platform SBM, and at least 220 million naira (\$530,000; £410,000) paid out as ransoms [and that] the Nigerian government reportedly paid 3 million euro (\$3.3 million; £2.4 million) to Boko Haram as ransom for the Chibok girls freed in negotiations.”²²

HT for the removal of organs

Reuters reported that a document from IS retrieved by the U.S. Special Forces in the Syrian Arab Republic justified the harvesting and removal of organs of “infidels,” stating, “The apostate’s life and organs do not have to be respected and may be taken with impunity.”²³ According

to data disclosed by the Director General of the Syria Coroner’s Office in November 2016, “More than 25,000 surgical operations were performed in the refugee camps of neighboring countries and [IS-controlled] areas in Syria since 2011 to remove the organs of 15,000 Syrians and sell them on the black market, according to a news outlet.”²⁴ It is worth highlighting that Interpol expressed concerns of trafficking for the removal of organs in North and West Africa, where impoverished communities and displaced populations (e.g., migrants, asylum seekers and refugees) are at greater risk of exploitation. Interpol also mentioned, “There is a wide spectrum of key actors involved in [trafficking in human beings for organ removal] in North and West Africa with connections to several countries on the continent and beyond, particularly in Asia and the Middle East.”²⁵

CONCLUSION

Disrupting and dismantling the financial flows of HT and terrorist networks is essential in order to combat these threats. Without human and financial resources, the capability and activity of terrorist organizations are degraded. As CTED points out, “Following the money could help disrupt potential exploitation networks, strengthen the detection of victims, and help bring perpetrators to justice.”²⁶ As a result, the financial sector and particularly financial intelligence units play a key role in the analysis of financial flows and transactions that may be linked to HT cases that support or finance terrorist organizations. Although it can constitute a significant challenge for financial institutions (FIs) to identify activity related to HT in the context of terrorist organizations, there are publications discussing and addressing these issues. Among the main resources available, FATF set out a list of recommendations as well as indicators and red flags pertaining to HT in general and OSCE synthesized financial indicators and red flags extracted from various resources.²⁷ In the same regard, FATF and FINTRAC set out lists of recommendations or indicators and red flags pertaining specifically to terrorist financing.²⁸ These risk indicators and red flags, as well as the cited resources in this article, can further strengthen FIs’ capacity to detect illicit flows deriving from HT and to prevent terrorist organizations from accomplishing their overall objectives and most importantly committing serious human rights violations. **AT**

Jonathan Dupont, FIU investigator and subject-matter expert on cryptocurrency, human trafficking and crimes against children, Lithuania, jonathandupont@protonmail.com

- ¹ "The Nexus Between Terrorism and Human Trafficking," *ACAMSToday.org*, January 17, 2023, <https://www.acamstoday.org/the-nexus-between-terrorism-and-human-trafficking/>
- ² "Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)," *Financial Action Task Force*, 2015, <https://www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html>
- ³ Nikita Malik, "Trafficking Terror: How Modern Slavery and Sexual Violence Fund Terrorism," *Henry Jackson Society*, 2017, <https://henryjacksonsociety.org/wp-content/uploads/2017/10/HJS-Trafficking-Terror-Report-web.pdf>
- ⁴ "Trafficking in Human Beings and Terrorism: Where and How They Intersect," *Organization for Security and Co-operation in Europe*, July 8, 2021, <https://www.osce.org/cthb/491983>
- ⁵ "Identifying and exploring the nexus between human trafficking, terrorism, and terrorism financing," *United Nations Security Council Counter-Terrorism Committee Executive Directorate*, 2019, <https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/files/documents/2021/Jan/ht-terrorism-nexus-cted-report.pdf>
- ⁶ "They came to destroy": ISIS Crimes Against the Yazidis," *Independent International Commission of Inquiry on the Syrian Arab Republic*, June 15, 2016, https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/ColSyria/A_HRC_32_CRP2_en.pdf
- ⁷ "Identifying and exploring the nexus between human trafficking, terrorism, and terrorism financing," *United Nations Security Council Counter-Terrorism Committee Executive Directorate*, 2019, <https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/files/documents/2021/Jan/ht-terrorism-nexus-cted-report.pdf>
- ⁸ "Report of the Secretary-General on conflict-related sexual violence," *United Nations Security Council*, 2018, <https://www.un.org/sexualviolenceinconflict/wp-content/uploads/report/s-2018-250/SG-REPORT-2017-CRSV-SPREAD.pdf>
- ⁹ Nikita Malik, "Trafficking Terror, How Modern Slavery and Sexual Violence Fund Terrorism," *The Henry Jackson Society*, 2017, <https://henryjacksonsociety.org/wp-content/uploads/2017/10/HJS-Trafficking-Terror-Report-web.pdf>
- ¹⁰ "The Islamic State Is Forcing Women to Be Sex Slaves," *The New York Times*, August 21, 2015, <https://www.nytimes.com/2015/08/21/world/middleeast/the-islamic-state-is-forcing-women-to-be-sex-slaves.html>
- ¹¹ J. G. Horgan et al., "From Cubs to Lions: A Six Stage Model of Child Socialization into the Islamic State," *Studies in Conflict & Terrorism*, 2016, https://www.researchgate.net/publication/305923601_From_Cubs_to_Lions_A_Six_Stage_Model_of_Child_Socialization_into_the_Islamic_State
- ¹² "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," *Financial Action Task Force*, March 2012, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>
- ¹³ "Terrorist Financing in West Africa," *Financial Action Task Force*, October 2013, <https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/tf-west-africa.html>
- ¹⁴ "Financial Flows from Human Trafficking," *Financial Action Task Force*, July 2018, <https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/human-trafficking.html>
- ¹⁵ "Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)," *Financial Action Task Force*, 2015, <https://www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html>
- ¹⁶ "They came to destroy": ISIS Crimes Against the Yazidis," *Independent International Commission of Inquiry on the Syrian Arab Republic*, June 15, 2016, https://www.ohchr.org/Documents/HRBodies/HRCouncil/ColSyria/A_HRC_32_CRP2_en.pdf
- ¹⁷ Ibid.
- ¹⁸ Mogos O Brhane, "Trafficking in Persons for Ransom and the Need to Expand the Interpretation of Article 3 of the UN Trafficking Protocol," *Anti-Trafficking Review*, Issue 4, 2015, pp. 120-141, <https://www.antitraffickingreview.org/index.php/atrjournal/article/view/93/113>
- ¹⁹ "Identifying and Exploring the Nexus Between Human Trafficking, Terrorism, and Terrorism Financing," *United Nations Security Council Counter-Terrorism Committee Executive Directorate*, 2019, <https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/files/documents/2021/Jan/ht-terrorism-nexus-cted-report.pdf>
- ²⁰ Ibid.
- ²¹ "Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," *United Nations Security Council*, January 29, 2016, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/231/80/PDF/N2223180.pdf?OpenElement>
- ²² "Nigeria's Chibok girls: Why was this former captive treated differently?" *BBC News*, April 17, 2022, <https://www.bbc.com/news/world-africa-61092882>
- ²³ "Exclusive: Islamic State sanctioned organ harvesting in document taken in U.S. raid," *Reuters*, December 24, 2015 <https://www.reuters.com/article/us-usa-islamic-state-documents-idUSKBN0U805R20151225>
- ²⁴ "International Partnerships Among Health, Private Sector, and Law Enforcement Necessary to Mitigate ISIS's Organ Harvesting for Terrorist Funding," *Joint Counterterrorism Assessment Team*, May 11, 2017, <https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/First-Responders-Toolbox---International-Partnerships-Among-Public-Health-Private-Sector-and-Law.pdf>
- ²⁵ "North and West Africa: INTERPOL report highlights human trafficking for organ removal," *Interpol*, September 30, 2021, <https://www.interpol.int/en/News-and-Events/News/2021/North-and-West-Africa-INTERPOL-report-highlights-human-trafficking-for-organ-removal>
- ²⁶ "Identifying and Exploring the Nexus Between Human Trafficking, Terrorism, and Terrorism Financing," *United Nations Security Council Counter-Terrorism Committee Executive Directorate*, 2019, <https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/files/documents/2021/Jan/ht-terrorism-nexus-cted-report.pdf>
- ²⁷ "Following the Money: Compendium of Resources and Step-by-step Guide to Financial Investigations Into Trafficking in Human Beings," *Organization for Security and Co-operation in Europe*, November 7, 2019, <https://www.osce.org/cthb/438323>; "Financial Flows from Human Trafficking," *Financial Action Task Force*, July 2018, <https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/human-trafficking.html>
- ²⁸ "Terrorist Financing in West Africa," *Financial Action Task Force*, October 2013, <https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/tf-west-africa.html>; For indicators specifically related to terrorist financing please visit: "Money laundering and terrorist financing indicators—Money services businesses," *FINTRAC*, https://fntrac-canafe.canada.ca/guidance-directives/transaction-operation/indicators-indicateurs/msb_mltf-eng#s10

Geographical battles

Political motivations

Financial gain

Religious ideologies

Racial tensions



FinCEN's TERRORIST FINANCING POLICIES

The article titled "FinCEN's AML and Terrorist Financing Priorities: An Introduction,"¹ featured in the *ACAMS Today* 12th Law Enforcement Edition, shared general thoughts, basic definitions and practical examples on each of the national anti-money laundering (AML) priorities. This article, the fifth of the series, will discuss terrorist financing in greater detail.

As mentioned in the introductory article, terrorist activities are violent acts or criminal activity (not necessarily linked to violence) committed by individuals and/or groups to coerce a government or its citizens to further certain political or social objectives. Terrorism is a global problem and while there is not a universally accepted definition for terrorism, these acts pose significant challenges both domestically and abroad as terrorists pursue their ideals. The U.S. Federal Bureau of Investigation (FBI) defines terrorism in a similar manner: The use of violence and intimidation in the pursuit of political, social or ideological aims. While these issues seem to be clear, when you apply an AML lens to this priority, it gets quite complicated. As mentioned before, it is important to recognize that there are specific reporting requirements for certain terrorist finance violations that could require immediate action from reporting/regulated entities.²

Why is terrorism one of FinCEN's national priorities?

Counter-terrorist financing (CTF) became a global priority as a result of the terrorist attacks of September 11, 2001 (9/11). An immediate response following the 9/11 attacks came by way of the global freezing of assets of known terrorists, an action supported by the G-7, an intergovernmental political forum consisting of Canada, France, Germany, Italy, Japan, the U.K. and the U.S.

This initial effort has evolved. Although there is no universal definition for terrorism, over the last 21 years, we have experienced and witnessed a global commitment in the way of enhanced regulations, legislation, policies and global recommendations. This effort involves a shared understanding of terrorist financing and how it differs from money laundering. Although they both involve the exploitation of the legitimate financial sector to further criminal activity, they are, in fact, different, with different levels of complexity and typologies.

One such difference is the fact that terrorist financing uses legitimate funds to further terrorist activities. That is to say that the source of funds could be hard-earned monies. Nevertheless, terrorist organizations are known to use several techniques to obscure the ultimate use of the funds (the crime) while protecting their supporters and the legitimate source of the funding. In contrast, money laundering, by definition, involves the proceeds of illegal activities. The purpose of money laundering is to give the illicit proceeds the appearance of legitimacy, thus allowing criminals to further their illicit enterprise and acquire goods and services in a seemingly legitimate fashion. Terror networks and/or lone wolf terrorists often use similar processes, products and services to obscure the ultimate user/use of the funds. Another key difference between money laundering and terrorist financing is the amount of the monies being moved through the financial system. While traditional money laundering schemes are mostly large in volume, terrorist finance activities could involve small payments and funding support to pay for items that could be aligned with the stated purpose of an account, such as funding to cover living expenses like rent, utilities, groceries, college, etc. Some factors to consider when analyzing suspected terrorism financing activity include:

- The source of the funds
- The flow of the funds
- Whether the funds are used for the intended purpose
- Deviations from customer financial patterns. Terrorist operators and cells are known for going dormant for long periods of time (sometimes years). Thus, sudden changes in financial behavior are a key indicator

Terrorism and its financing are continuously evolving, and terrorists are known for leveraging every tool available to support their harmful goals



Evolution of terrorist financing

Often people hear the word terrorism and immediately think of violent attacks or individuals that are not educated; that is not always the case. Keep in mind that Ayman al-Zawahiri was an eye surgeon. Terrorism and its financing are continuously evolving, and terrorists are known for leveraging every tool available to support their harmful goals. For example, on August 13, 2020, the U.S. Department of Justice released a news statement announcing the global disruption of three terror finance cyber-enabled campaigns.³ These terror finance campaigns relied on sophisticated cyber tools, including donations in cryptocurrency. The investigative team uncovered that the terror groups were leveraging technology and conducting complex financial transactions, including the handling of cryptocurrency.

Al-Qassam Brigades campaign

Since 2019, the Al-Qassam Brigades have been seeking donations from supporters via bitcoin to fund their terrorist campaign. Their website even included video instructions on how to anonymously make such donations and further set up multiple cryptocurrency accounts to support their efforts.

Al-Qaeda campaign

Al-Qaeda and affiliated groups operated a bitcoin money laundering network using Telegram channels and other social media platforms to solicit cryptocurrency donations to support their terrorist activities. They even presented themselves, in some cases, as charitable organizations while, in fact, openly soliciting funds for terrorist activity, including providing equipment to terrorists in Syria. It was later uncovered that these terror groups used complicated obfuscation techniques to layer their transactions, thus concealing their actions.

Islamic State group campaign

The third campaign under this indictment illustrates how terrorists evolve and are nimble and adaptable. This last funding campaign by an Islamic State group facilitator, that among other things, managed Islamic State group hacking operations, involved selling fake personal protective equipment (PPE) during the COVID-19 pandemic. The website claimed to sell Federal Drug Administration-approved N95 respirator masks when, in fact, they were not legitimate masks.

Another notable example of attacks or terrorist activities not involving violence is distributed denial of service (DDOS) attacks, which are malicious online attempts to disrupt legitimate and essential websites (hospitals, schools, service providers) or to interfere with the distribution of utilities or electricity plants. For example, and as mentioned in the previous article within this series, in May 2021, many drivers were stranded on U.S. East Coast highways, unable to refuel their vehicles due to unexplained gasoline shortages. Almost immediately, it was revealed that the Colonial Pipeline, a major East Coast fuel pipeline, was shut down by criminals. This attack represents the most significant cyberattack on U.S. energy infrastructure.

As illustrated above, different criteria can be used to define terrorism, whether driven by political, social or ideological causes. Their motivations could be different, including:

- Religious ideologies
- Political motivations
- Racial tensions
- Financial gain
- Geographical battles

Terrorist networks are nimble, adaptable and highly sophisticated. While they are vastly different due to their ideologies, means, methods, size, scope or complexity, terrorist organizations are well organized, with some operating under a corporate-like structure that includes a specific mission/ideal, unique infrastructure, funding efforts/sources/mechanisms and operations.

Conclusion

In order to carry out their attacks, whether violent or not, terrorist networks must have access to continued funding to further their goals and perform their activities. Therefore, identifying and disrupting their ability to raise, store, move and use funds translates into dismantling their operations and objectives, thus efficiently stopping terrorist activities from affecting global stability. CTF is a shared global responsibility, and we are all part of the effort.

Some key red flags for detecting terrorist financing are as follows:

- Multiple individuals sending structured payments to an individual/account in a known jurisdiction for terror activity or terror safe haven
- Cash deposits and withdrawals in/out of accounts owned by charitable organizations
- High-risk individuals receiving funds from an unknown source
- Know your customer information is unavailable for the originator of a wire transfer to/from high-risk jurisdictions. **AT**

Raymond Villanueva, CAMS, director, Risk Advisory Services, Kaufman Rossin, FL, USA, rvillanueva@kaufmanrossin.com

¹ Ray Villanueva, "FinCEN's AML and Terrorist Financing Priorities: An Introduction," *ACAMS Today* June-August 2022, Vol. 21 No. 3, <https://www.acamstoday.org/fincens-aml-and-terrorist-financing-priorities-an-introduction/>

² For additional information, please visit 31 CFR §§ 1020.320 (banks); 1021.320 (casinos and card clubs); 1022.320 (money services businesses); 1023.320 (brokers or dealers in securities); 1024.320 (mutual funds); 1025.320 (insurance companies); 1026.320 (futures commission merchants and introducing brokers in commodities); 1029.210 (loan or finance companies); and 1030.210 (housing government-sponsored enterprises).

³ "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," *U.S. Department of Justice*, August 13, 2020, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>

IS IT "GROUNDHOG DAY" FOR DIGITAL ASSETS?



2022 was a rollercoaster year for digital asset regulation and enforcement—at times fluctuating between a “Groundhog Day”-esque barrage of been-there-before and an endless array of shock and awe. Like every February when our stout-bodied rodent friend prepares to pop out of his hole, the question looms, will this year be a different kind of year for digital assets—an early spring, if you will—or does Punxsutawney Phil have us destined for a longer crypto winter?

Continued regulatory response to hacks

2022 was a record-setting year for hacks. It was easy to feel, at times, like Bill Murray’s cynical weatherman as hundreds of millions of dollars in cryptocurrency were stolen from cryptocurrency businesses at alarming speed and scale on a regular basis. According to TRM analysis, 2022 was an unparalleled year for crypto hacks, with about \$3.7 billion in stolen funds.¹ Attacks against decentralized finance (DeFi) projects were particularly common, with approximately 80% of all stolen funds, or \$3 billion, involving DeFi-related victims.²

While in the age of the internet, a hack meant the loss of usernames and passwords, in the age of crypto, a hack means the loss of life savings. It also means that stolen funds can be used directly by nation-state actors like North Korea to fund weapons proliferation and other destabilizing activity. For example, the year’s largest hack was perpetrated on March 23 by North Korea’s Lazarus Group against the Ronin bridge—an infrastructure attack on a bridge associated with the play-to-earn game Axie Infinity.³ North Korean cybercriminals stole over \$600 million in cryptocurrency. While North Korea has long engaged in cyberattacks on cryptocurrency businesses to raise funds to subsidize its weapons programs, nuclear proliferation and other destabilizing activities, the Ronin hack was unprecedented.

In the wake of the proliferation of hacks and other exploits, we also saw regulatory action. That action took a number of forms. First, we saw the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) use sanctions to go after threat

actors. For example, following the attack on the Ronin bridge, OFAC used blockchain intelligence to trace the stolen funds. Once found, OFAC sanctioned both the blockchain addresses to which the funds moved and the mixing services that North Korean cyber criminals utilized to launder over a billion dollars of cryptocurrency—including centralized bitcoin mixer blender.io and decentralized ethereum mixer Tornado Cash. While the sanctions against Tornado Cash raised questions of privacy vs. security and became one of the biggest stories of 2022, these sanctions are also an example of how regulators—for better or worse—attempted to address the hacking epidemic.

In 2023 we will likely continue to see a litany of attacks on cryptocurrency businesses—as the decentralized ecosystem continues to catch up with cybercriminal threats—and a continued regulatory and law enforcement (LE) response. A two-stage approach must be taken to mitigate the risks to DeFi protocols and wider crypto-enabled crime. First, hacks can only be stopped by improving cyber security at DeFi protocols and other cryptocurrency businesses. Improving cyber security can be done by continued emphasis on public-private coordination to ensure cryptocurrency businesses are engaging in cybersecurity best practices. In doing so, they will make themselves less vulnerable to hacks. Second, we must make these hacks and crypto-enabled crime less profitable by increasing friction in the money laundering process. This means ensuring that LE has the advanced compliance tools and training they need to track and trace funds in an attempt to seize them back from threat actors.

Bill Murray and Andie MacDowell, stars of the 1993 film “Groundhog Day.”



2023 is becoming a year for anti-money laundering (AML)-related enforcement actions

In 2023 we are already seeing a continued emphasis on enforcement actions as policymakers globally work on comprehensive frameworks for digital assets.

In January, only a few weeks into 2023, the U.S. Department of Justice⁴ (DOJ) and the U.S. Treasury Department⁵ announced a coordinated action against noncompliant Hong Kong-registered cryptocurrency exchange Bitzlato and the arrest of its owner for “conducting a money transmitting business that transported and transmitted illicit funds and that failed to meet U.S. regulatory safeguards, including anti-money laundering requirements.” The actions directly linked Bitzlato to illicit Russian finance—particularly, ransomware and dark web markets—allowing the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) to issue for the first time an order pursuant to section 9714(a)⁶ of the Combating Russian Money Laundering Act. This order designated Bitzlato as a “primary money laundering concern” in connection with illicit Russian finance and prohibited certain transmittals of funds involving Bitzlato by any covered financial institution.

As explained in the DOJ release, “As a result of deficient know-your-customer (KYC) procedures, Bitzlato allegedly became a haven for criminal proceeds and funds intended for use in criminal activity. Bitzlato’s largest counterparty in cryptocurrency transactions was Hydra Market, an anonymous, illicit online marketplace for narcotics, stolen financial information, fraudulent identification documents and money laundering services that was the largest and

longest-running dark web market in the world. Hydra Market users exchanged more than \$700 million in cryptocurrency with Bitzlato, either directly or through intermediaries, until Hydra Market was shuttered by U.S. and German LE in April 2022. Bitzlato also received more than \$15 million in ransomware proceeds.”⁷

The Bitzlato action was significant for a number of reasons. First, it built on prior actions against Russian illicit finance in the crypto space taking out another noncompliant virtual asset service provider that allowed illicit finance to move unabated. Adding to actions against SUEX, Chatex and Garantex—not to mention dark web mixers Helix and Bitcoin Fog—the Bitzlato action was also notable for the breadth of global LE cooperation with France, the Netherlands and Europol playing significant roles in taking down Hydra’s payment service of choice.

Most notable, perhaps for the ACAMS community, is the emphasis on AML. The DOJ complaint highlights, at every turn, Bitzlato’s proactive disregard for AML controls. According to DOJ, Bitzlato has marketed itself as requiring minimal identification from its users, specifying that “neither selfies nor passports [are] required... As a result of these deficient know-your-customer (KYC) procedures, Bitzlato allegedly became a haven for criminal proceeds and funds intended for use in criminal activity,” including \$700 million in transactions with sanctioned dark web market Hydra and \$15 million in ransomware proceeds. DOJ and the U.S. Department of the Treasury’s focus on Bitzlato’s lack of AML controls is an attempt to take a bad actor—particularly one that is facilitating Russian illicit finance—out of the financial system, but it is also sending a clear message to other exchanges that authorities expect robust AML controls.



During a news conference in January 2023, Kenneth Polite, assistant attorney general for the Department of Justice’s Criminal Division, addresses the arrest of the majority shareholder and founder of virtual currency exchange Bitzlato Ltd. for allegedly transporting and transmitting hundreds of millions of dollars in illicit funds. Photo by Daphne Psaledakis/Reuters

Expect even more from the White House

While we may see some action from the U.S. Congress on cryptocurrency legislation in 2023, the fractured political environment will likely elicit “Groundhog Day” comparisons to 2022 with a hurry-up-and-wait approach to digital assets legislation. That means we are likely to continue to see more enforcement actions and guidance from regulators like the U.S. Securities and Exchange Commission, the Commodity Futures Trading Commission and the U.S. Department of the Treasury. In 2022, we saw a White House executive order on cryptocurrencies⁸ and the first-ever framework for digital assets.⁹


Already in 2023, we have seen the White House issue a “roadmap”¹⁰ to mitigate cryptocurrencies’ risks which, among other things, calls on Congress to “step up its efforts” on digital assets legislation. The roadmap, which encourages more enforcement actions and guidance from regulators and calls for additional efforts in the AML space, states that “In the coming months, the Administration will also unveil priorities for digital assets research and development, which will help the technologies powering cryptocurrencies protect consumers by default.” This could preview coming work on digital identity or other technological solutions to what the White House may see as challenges for compliance in a more decentralized cryptocurrency ecosystem.

In 2023 we are already seeing a continued emphasis on enforcement actions as policymakers globally work on comprehensive frameworks for digital assets

Focus on the challenges and opportunities in the DeFi ecosystem

As we look around the globe, this is the most fundamental question for policy-makers as we all embark on a journey into a more and more decentralized world. While over the last few years, regulators have been focused on how to regulate centralized exchanges—think the travel rule and how exchanges engage with self-hosted wallets—global policymakers will be focusing more on what regulation can and should look like in a more decentralized world. For example, the recent White House framework for digital assets tasked the U.S. Department of the Treasury with completing an illicit finance risk assessment on decentralized finance by the end of February 2023 and an assessment on non-fungible tokens by July 2023. While we have seen some guidance from the Financial Action Task Force (FATF)—which has proposed an owner/operator test to determine whether a decentralized exchange may have certain AML obligations—we have not seen much from global regulators when it comes to DeFi.

That could change as we emerge from our burrows into spring 2023. We also will likely see a continued emphasis on consumer and investor protection, advertising and separation of funds in the wake of FTX, with the New York Department of Financial Services providing January regulatory guidance¹¹ to protect consumers in the event of a virtual currency insolvency. The guidance, among other things, called for New York-licensed entities to segregate and limit the use of customer funds.

This means that 2023 is already gearing up to be a busy year in the crypto verse. We will likely see more hacks, more enforcement actions, more guidance and much more. But predictions are hard—in crypto and the weather. Just ask our furry friend Punxsutawney Phil. 

Ari Redbord, TRM Labs, Washington, D.C., ari@trmlabs.com

¹ “Looking Back at 2022 and Towards 2023 to See What the Future Holds for Digital Assets Policy,” *TRM Labs*, December 29, 2022, <https://www.trmlabs.com/post/looking-back-at-2022-and-towards-2023-to-see-what-the-future-holds-for-digital-assets-policy>

² *Ibid.*

³ “North Korea’s Lazarus Group moves funds through Tornado Cash,” *TRM Labs*, April 28, 2022, <https://www.trmlabs.com/post/north-koreas-lazarus-group-moves-funds-through-tornado-cash>

⁴ “Founder and Majority Owner of Bitzlato, a Cryptocurrency Exchange, Charged with Unlicensed Money Transmitting,” *U.S. Department of Justice*, January 18, 2023, <https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money>

⁵ “Remarks by Deputy Secretary of the Treasury Wally Adeyemo on Action Against Russian Illicit Finance,” *U.S. Department of the Treasury*, January 18, 2023, <https://home.treasury.gov/news/press-releases/jy1193>

⁶ “FinCEN Identifies Virtual Currency Exchange Bitzlato as a ‘Primary Money Laundering Concern’ in Connection with Russian Illicit Finance,” *Financial Crime Enforcement Network*, January 18, 2023, <https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering>

⁷ “United States of America - Against - Anatoliy Legkodymov, also known as ‘Anatolii Legkodymov,’ ‘Gandalf’ and ‘Tolik,’ Defendant,” *U.S. Department of Justice*, <https://www.justice.gov/usao-edny/press-release/file/1562996/download>

⁸ “Executive Order on Ensuring Responsible Development of Digital Assets,” *The White House*, March 9, 2022, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/>

⁹ “FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets,” *The White House*, September 16, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/>

¹⁰ “The Administration’s Roadmap to Mitigate Cryptocurrencies’ Risks,” *The White House*, January 27, 2023, <https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks/>

¹¹ “Virtual Currency Guidance,” *New York State Department of Financial Services*, January 23, 2023, https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230123_guidance_custodial_structures



INFORMATION SHARING:

WHY COMMUNITY BANKS SHOULD PARTICIPATE

Section 314 of the USA PATRIOT Act, which was passed back in 2001, is a vital portion of the legislation. Anyone who had been in the anti-money laundering/Bank Secrecy Act (AML/BSA) space prior to 2001 understands how significant this change was to the industry. Section 314 specifically centered around the ability of financial institutions (FIs) and law enforcement (LE) to share information. In the shadow of the terrorist attacks that occurred on September 11, 2001, the federal government wished to address possible loopholes utilized by terrorists and other threat actors who used the U.S. financial system.

Section 314(a) and (b)

The two portions of Section 314 are "a" and "b." Section 314(a) centered around required information sharing with LE, while Section 314(b) concerns voluntary sharing between FIs. Often, a voluntary provision of regulation leads to one of two trains of thought. One is that it is voluntary, thus making it not worth a banker's time to deal with as there are plenty of other "required" items to occupy our time. The other is that even though it is voluntary, the bank is "compelled" to participate for fear of possible scrutiny for not doing so.

While 314(b) is voluntary, it is important that all community banks participate, not because they feel compelled but rather for the role they can play in assisting LE and each other in deterring financial crime. Originally, when the PATRIOT Act was passed, it was stated that information sharing should be used only for activity related to terrorist financing and/or money laundering. Many felt that this left a narrow scope to employ the information-sharing tool. Given the litigious nature of our society, FIs may have felt that it was not worth the risk for fear of sharing something that was not covered under the scope of the act.

Clarification

Due to concerns conveyed by FIs, the Financial Crime Enforcement Network (FinCEN) issued a Section 314(b) Fact Sheet in November 2016 that replaced and rescinded previous guidance issued in 2009 and a 2012 administrative ruling. This new fact sheet provided further clarification on what FinCEN considered appropriate sharing requirements. A further amended fact sheet was released in December 2020. The guidance reiterated the safe harbor created by Section 314(b) to protect those institutions that choose to share. It also spoke to specified unlawful activities (SUAs),



which are predicate crimes that apply to a money laundering offense. The SUAs listed in 18 U.S.C. subsection 1956 include a wide variety of fraud and other criminal activities such as fraud against individuals, organizations, governments, computer fraud and abuse or other financially motivated crimes. The guidance also states that an FI does not need to have specific information indicating that activity is directly related to an SUA or have even reached a conclusion that activity is suspicious in order to share and receive safe harbor. It should also be noted that there are no limitations on sharing personally identifiable information under section 314(b). The information can be shared both in writing or verbally and it is expected that regardless of the method used, the FI maintains appropriate procedures to protect the confidentiality of all information shared.

One limitation that is in place is the prohibition of directly sharing a suspicious activity report (SAR) with another FI or disclosing information that would reveal the existence of a SAR. The confidentiality of these documents remains paramount to FinCEN. While the existence of an existing SAR is not permissible, 314(b) provides an avenue for FIs to file joint SARs through the use of the provision.

This clarification of FinCEN's ideal for 314(b) truly outlines how and why they wish for FIs to use it. Let us examine some reasons why a community bank may choose not to utilize 314(b) and some counterarguments to those reasons:

- 1. It is not worth the time and effort and is only voluntary.** While no one would argue that there is always plenty of work to be done and voluntary items are lower on the priority list, I would argue that the professionals in the AML/BSA space care deeply about what they do and the core of our mission is to help fight and deter financial crimes. The sharing of information between institutions can be a powerful tool in helping achieve that goal.
- 2. Even if we choose to participate, other banks may ignore or will not share back.** If you have worked with 314(b) in any capacity over the years, you have undoubtedly come across one or more banks that never seem to respond to any inquiries. While that can be frustrating, one never knows which banks will or will not respond. Thus, going back to our mission of helping fight and deter financial crime, it is important to participate via the

"two-way street" to help others and ourselves in being able to further connect the dots on financial crime.

- 3. We are afraid to share "the wrong thing."** This was a common area of concern during the earlier days of 314(b). However, as outlined above, FinCEN has taken great care to show FIs that they wish to encourage sharing and wish to dispense with barriers that might otherwise prohibit banks of all sizes from participating. Any effort made in good faith to use the tool appropriately will not be punished.

Conclusion

To summarize, information sharing can be a powerful tool to help community banks fight the good fight against criminal elements. FinCEN has done a good job of clarifying to remove barriers to sharing. Like any fight, it is better to have allies to rely on and this tool is a great way of developing allies across the industry. If your institution does not actively participate now, please give thought to registering and participating going forward. AT

Carl Francois, senior vice president, BSA and fraud officer, Southern First Bank, LinkedIn

REGULATORY AMBIGUITY IN INDIA—

BREEDING GROUND FOR CRYPTO CRIMINALS



When Satoshi Nakamoto penned the original white paper introducing the world to bitcoin and blockchain technology, no one had ever imagined that virtual currencies or cryptocurrencies would bring a tsunami of changes in the world of digital technology and financial services. Since its first use in 2009, there are approximately 300 million crypto users across the world as of 2021.¹ India is estimated to have more than 100 million users,² distinguishing it as the country with more cryptocurrency users than any other and placing India in the league of countries at the forefront of absorbing new technology and adopting innovation. This has been acknowledged by India's key regulator—The Reserve Bank of India (RBI)—as well.



A monument to Satoshi Nakamoto, the mysterious founder of Bitcoin, was created by Reka Gergely and Tamas Gilly for a park in Budapest, Hungary.

Despite being recognized as the world's largest user of crypto, India still needs to catch up in terms of providing regulatory clarity and the necessary directives for recognizing cryptocurrency. The April 2018 notification by RBI on the prohibition on dealing in virtual currencies and the subsequent verdict by the Supreme Court of India overruling that notification indicates the state of regulatory ambiguity in India. This verdict turned out to be a key game changer as it not only exacerbated the confusion around using cryptocurrency but also triggered a spate of headaches for the RBI in terms of not providing the necessary guidelines to the regulated entities—as well as instances where cryptocurrency has been used as a conduit for carrying out fraud and money laundering activities.

Regardless of the lack of regulatory framework, Indians are still drawn to the use of cryptocurrencies, usually unaware of the related risks and worrying growth in the number of instances of money laundering involving cryptocurrency.

Global cryptocurrency regulations—A siloed approach

Currently, the existing regulations in India are at various maturity levels in terms of receptivity and building the regulatory framework to regulate the usage of cryptocurrencies. Countries like the U.S., Singapore and El Salvador are already at an advanced maturity level in terms of having the necessary regulations in place. However, countries like India are still contemplating how to accept cryptocurrencies and build regulations around them. Although the overall aim and approach are toward financial stability, preventing misuse and criminalization, and promoting innovation, the lack of coordination among all countries is still one of the biggest challenges to having robust and strong regulations.

Indian cryptocurrency regulation and its evolution

In 2013, RBI cautioned the general public regarding cryptocurrency, advising individuals not to deal with it considering the risk involved, the potential misuse of cryptocurrency and the absence of any regulatory or legal framework. However, as cryptocurrency gained popularity at a global level, its misuse became widespread in India, primarily because of the absence of crypto regulation. Although RBI reiterated its stance and issued many cautions to the public in addition to releasing follow-up notifications in 2017 and 2018 advising individuals not to deal in cryptocurrencies, there was no concrete development on the formulation of crypto regulation.

Cryptocurrency scams and select case studies

To understand the impact of the absence of appropriate crypto regulations and the legislative framework, one must examine the various scams that have occurred in India over the past two decades. These fraud and money laundering instances can also act as a case study for the academic circle and will clearly demonstrate how the absence of a legislative framework, coupled with a low level of education and greed, can result in major scams that penetrate the social structure where employment and poverty is a major issue even in the 21st century.

Although this article focuses on recent scams, the most prominent of these crimes, as per the analysis of information available in the public domain, is the GainBitcoin Scam, which occurred from 2014 to 2018. The scam involved Amit Bhardwaj, Ajay Bhardwaj and Vivek Bhardwaj as the accused. Other prominent

older schemes included the Bitconnect, Regal Coin and Dekado Coin scams, all of which involved Divyesh Darji as the key person accused.

One of the more recent scams is the 2020 scam in which the public was defrauded after being lured into investing in Morris Coin by businessman Nishad K., who promised investors a daily return and other bonuses for each referral to a multi-level marketing chain that turned out to be a Ponzi scheme. Nishad K. duped nearly 900 investors under the guise of an initial coin offering through his companies Long Rich Global, Long Rich Technologies and Morris Trading Solutions. The case is still under investigation; however, the mastermind is at large.

Another recent instance of a crypto scam is the Ether Trade Asia scam, which operated from 2020 to 2021, posing as a trading platform that promised daily returns to the tune of 3%.³

Apart from these scams and Ponzi schemes, in November 2022, law enforcement authorities identified the involvement of cryptocurrency in money laundering cases via crypto exchanges. One such instance, via information available in the public domain, is the investigation against one of the world's largest crypto exchanges, which was accused of involvement in money laundering estimated at \$500 million⁴ after the investigating agencies discovered the anonymous remittance of illegal cash and no details of the beneficiaries.

Another recent instance that was brought to public notice, occurring in June 2022, was a fraud worth \$150 million.⁵ In this scheme, fraudsters duped the public by posing as fake exchanges. These tech-savvy criminals used fake domains and social media accounts to contact and convince users into investing in fake exchanges. Once the investors were trapped and had invested their own money, the criminals approached them as investigative agents or posed as other investors to acquire important details such as credit card and bank account numbers. These details were then used to carry out other criminal activities. This scam is known as the "CoinEgg Scam."⁶

Cryptocurrency ecosystem— Key challenges

The multiple scams and the involvement of cryptocurrency in conducting money laundering activity in India have raised some serious questions for regulators and the government. Some of the key challenges that need to be tackled immediately are mentioned below.

Absence of a watchdog: One of the major reasons for slow investigations into cryptocurrency scams is the absence of a watchdog at a national level. Although the investigations are pursued by other investigative agencies, there needs to be a specialized watchdog or a national agency specializing in investigating cryptocurrency-related matters. As technology advances and criminals become more tech savvy, the necessity of such a specialized national agency is evident. Since such investigations require specialized investigation and technical skills, it will be prudent that such a national agency or watchdog office is established to focus only on cryptocurrency-related scams and related instances.

Revamped judicial system: The second challenge is related to the first one, and it involves the current judiciary system. The existing system is too old and not tech savvy. In addition, the absence of a legislative framework makes it easy for criminals to beat the system and avoid any legal actions against them. The scams mentioned above are classic examples where the mastermind or the prime accused could obtain bail and abscond even before legal proceedings were initiated against them. This demonstrates that the current judiciary system needs to get up-to-speed and become more tech savvy and digital, which will ensure that the legal framework is not skewed toward criminals and that the public also has faith that they will get quicker justice.

*One of the major reasons
for slow investigations into
cryptocurrency scams is
the absence of a watchdog
at a national level*



Upskilling the investigative agencies: The crypto ecosystem is a complicated system, and it is difficult to understand the nuances. The way criminals are advancing in terms of their knowledge and innovative techniques to defraud the public is leaving investigative agencies behind. They are not appropriately equipped in terms of knowledge level or providing the right tools to carry out such investigations. Therefore, cases fall into the cracks and investigations run for years without any concrete results. It is very important that investigative agencies are appropriately skilled and have the right kind of investigative tools to conclude investigations and restore public trust.

Enhanced public awareness: Going by the case studies mentioned above, one common theme is identified: The lack of knowledge. Innocent members of the public do not have an understanding of such scams or criminals and therefore fall victim to these crimes. For that reason, it is necessary that Indian government agencies take the initiative to increase public awareness.

Conclusion

The regulatory ambiguity regarding cryptocurrencies in India has resulted in a breeding ground for crypto criminals. For that reason, a swift call to action is needed within the country to establish a regulatory framework regarding cryptocurrencies. The case studies outlined in the article clearly demonstrate the urgency of establishing a legislative and regulatory framework if India wants to contain cryptocurrency-related scams and money laundering instances. There is already a lot of traction on the subject and these efforts need to be continuously pursued by various agencies under the auspices of the government. Although there is still no clarity as to who will regulate cryptocurrency in India, it all depends on if it will be treated as another asset class or a currency. As of now, RBI is taking the lead in terms of having oversight of the cryptocurrency space in India and may become a regulator if cryptocurrency is considered a currency. However, if the consensus turns out differently and the government agencies decide to treat cryptocurrency as another asset class, then the existing capital market regulator (i.e., the Securities and Exchange Board of India [SEBI]) will be the

strong contender for being the regulator. As the famous poet George Herbert said, "Where there is a will, there is a way." It is just a matter of time before India will develop strong crypto regulations and execute this phrase, both in letter and spirit, by having an appropriate legislative and regulatory framework around cryptocurrency soon. **AT**

Sachin Shah, CAMS, domain consultant, Tata Consultancy Services, Mumbai, India, shahmsachin@gmail.com, LinkedIn

¹ Jordan Tuwiner, "63+ Cryptocurrency Statistics, Facts & Trends," *Buy Bitcoin Worldwide*, January 1, 2023, <https://buybitcoinworldwide.com/cryptocurrency-statistics/#>

² Ibid.

³ Matti Williamson, "'Ether Trade Asia' Director, Nishid Wasnik Arrested over Crypto Scam," *Finance Magnates*, February 20, 2022, <https://www.financemagnates.com/cryptocurrency/ether-trade-asia-director-nishid-wasnik-arrested-over-crypto-scam/>

⁴ Pradeep Thakur, "Over RS 4,000cr laundered via cryptos unearthed by ED in 1 year," *Times of India*, November 27, 2021, <https://timesofindia.indiatimes.com/india/over-rs-4000cr-laundered-via-cryptos-unearthed-in-1-year/articleshow/87939180.cms>

⁵ Bhaswati Guha Majumder, "CoinEgg Scam: Indian Investors Have Lost as Much as Rs 1,000 Crore, Finds Study," *News 18*, June 22, 2022, <https://www.news18.com/news/tech/coinegg-scam-indian-investors-have-lost-as-much-as-rs-1000-crore-finds-study-5419273.html>

⁶ "Crypto scammers have reportedly stolen ₹1000 crore off Indian users by posing as fake exchanges," *Business Insider India*, June 21, 2022, <https://www.businessinsider.in/cryptocurrency/news/indian-investors-may-have-lost-almost-1000-crore-in-crypto-scam-according-to-a-new-report/articleshow/92358876.cms>

What does a recruiter do?

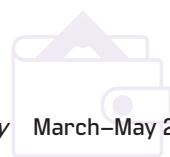
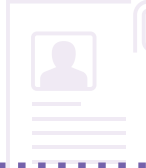
Many people have trouble understanding what employment recruiters are and what they do for a living. The irony is that what they do is actually simple—recruiters recruit. Some recruit nurses, while others recruit Java developers. Then there are those who recruit anti-money laundering (AML) and compliance professionals whose clients are financial services firms: traditional banks, cryptos, money services businesses, you name it.

Before we discuss the ins and outs of working with recruiters, we should start with a description of the general types of recruiters and how they work. There are two types: in-house and agency recruiters. In-house recruiters represent just one client: their company. An in-house recruiter at J.P. Morgan, for instance, recruits IT or compliance or customer service professionals only for J.P. Morgan. They get paid a base salary and bonus. The second type of recruiter works for an agency, vendor, a third party—whatever you would like to call them—and has many clients. Most agency recruiters are niched; they work on certain roles within specific industries. The two types of recruiters have the same end goal: To put the best talent in the right seat for their clients. You might not be the best candidate for their specific roles, but that does not mean you should not be open to dialogue with recruiters. I recommend speaking to all recruiters who work in your specific skill set and industry.

How and why to engage specific recruiters

Now would be a good time to discuss how you should use recruiters for your personal benefit. All recruiters are not created equal. You must vet, verify and try out recruiters just as you would vet contractors for house renovations, research the most appropriate credit card or investigate any type of service for which you are looking to register. However, you should





be sure to engage in-house recruiters and agency recruiters differently. They can help you out in unique ways, so it is best to communicate with them strategically, efficiently and with the right expectations.

- **In-house recruiters know their clients best.**
 - **Recruiters who work for one company are not eating what they kill.** Their jobs are to ensure they know their company's staffing strategy and culture and execute the game plan. Engage with in-house recruiters to learn more about a potential company's staffing plan, their short- and long-term needs, what it is like working there, the company's diversity, equity, and inclusion philosophy, and what roles they are looking to fill. If not for you, companies might have roles that are a better fit for friends and colleagues.
 - **Keep in touch. Your career is a long game.** In-house recruiters might not have roles that are a good fit now, but they might in the future. Take calls with in-house recruiters to discuss roles they are currently working on, but also with the goal of being considered for future roles. All recruiters remember the professionals that are open, interactive and helpful. In-house recruiters will also remember you when they move to a different company themselves.
 - **Always take their calls.** This feeds off the last bullet point but is worth more discussion. Speaking to recruiters does not mean you are betraying your current employer or are on the job market. Recruiters can use all the help they can get and are grateful to everyone who is willing to help. Take recruiter calls to get an understanding of what types of jobs are out there, what types of roles recruiters are working on and how to build a rapport with someone who might be able to help you in your career growth.

- **Agency recruiters know their markets best.**

- **Use them for intelligence.** Agency recruiters usually focus on one space and know that space both at the macro and micro levels. For instance, they recruit for AML and compliance roles in the financial service space or legal roles at law firms. Use agency recruiters as sources of information about your space, field and the job market.
- **Build long-term relationships.** Use them as advisors for both your career and immediate job search. Recruiters are great short-term solutions because they offer opportunities that might help you land a job or take the next step in your career trajectory. In the long term, recruiters can help you take multiple steps in your career or help you find a job when you get laid off for the first time (or the fifth time).

Words of wisdom

Some words of wisdom to apply when engaging recruiters: Use recruiters proactively and to your benefit. Most people passively engage recruiters—both in-house and agency—only when they are actively working on jobs that might be a good fit at any given moment. That strategy leaves a lot of valuable information and opportunity on the table. One of the best ways to take control is to have advisors and partners. Recruiters can be some of the best partners and advisors. Recruiters are essentially job agents that you get for free. So, run for the hills if a recruiter asks you for payment. No legitimate recruiter gets paid by a person on the job hunt or by potential candidates for one of their open jobs. Plus, some recruiters are better fits for your career growth than others, and you will get along with some recruiters better than others. It is always great to work with folks you like. Make sure you are vetting recruiters as much as they are vetting you because these business relationships should last as long as both of you share similar markets and industries. Here are some tips on how to use recruiters to your advantage:

- **Recruiters are therapists.** Agency recruiters regularly have calls with their best candidates and clients that are mostly about how poor their work environment is at that moment. Sometimes, the calls are about how great work is going. But often, we need to get rid of stress. Now, do not call a recruiter to de-stress all the time; they will stop picking up your calls. However, next time you are going to speak to a trusted recruiter to catch up or discuss a role, do not hold back on venting about work. It is usually a safe space. A recruiter works in your field without working at your company. And they are not part of your friends and family circle, so you do not have to worry about it getting too personal. It is a good judgment-free zone.

Some words of wisdom to apply when engaging recruiters: Use recruiters proactively and to your benefit



- **Knowledge is power.** In-house and agency recruiters like to talk about what they know. Use that to your advantage. If you are in the job market or thinking about the next steps in your career, trusted recruiters can provide insight into what they are seeing from their clients, which skill sets are in demand, who is hiring and who is not, etc. This is all valuable information that will help you set expectations around your ability to find your next role, compensation ranges and the time duration.
- **Sometimes it is whom you know (and whom you like).** Building strong relationships with recruiters can have great passive benefits. Recruiters are good agents to have on your side both while you are keeping your head down and working or if you are actively interviewing and seeking a job. They will reach out to you if they have a strong opportunity because you will be at the forefront of their mind. That is why it is recommended that you build relationships with multiple recruiters because they all work on different types of jobs with different clients. The probability of getting a call about the right role will only increase with the more relationships you have.
- **Networking is one of the ways to control your career.** Building relationships with recruiters is like networking on steroids. Agency recruiters are hustling to build relationships with hiring managers at companies. That means you are automatically piggybacking off their business development and networking. In-house recruiters are building relationships with line managers as their clients, and you will have access to those line managers as well. You do not always have to go to a happy hour or a conference to network.

Conclusion

It cannot be emphasized enough that advice from partnerships with and relationships with recruiters—the good, the bad, in-house or agency—are all free of charge. And engaging with recruiters proactively is one of the most efficient ways to gain control of your career. It is your responsibility to determine your career goals, develop a strategy and then formulate a plan. One of the tactics of that plan should be to build relationships with key recruiters in your space so you know when the best times and the worst times are to look for work and when the next job in your career trajectory is open and available.

Recruiters can work as your agents in your search and during the interview process, and they can be good advisors when you have an offer in hand or when you just need to complain about your current job. Finally, based on the law of averages, you will have more success if you have relationships with more recruiters. Having four to five go-to recruiters who have been with the same company or agency for at least three to five years is a great start. They need to recruit in your line of work, and you will need to speak to them (maybe more than once) to get an idea of whether they are knowledgeable or not. It will take time and a few dud calls, but it will benefit you greatly if you have sources of market intelligence you can tap into at any given time. **AT**

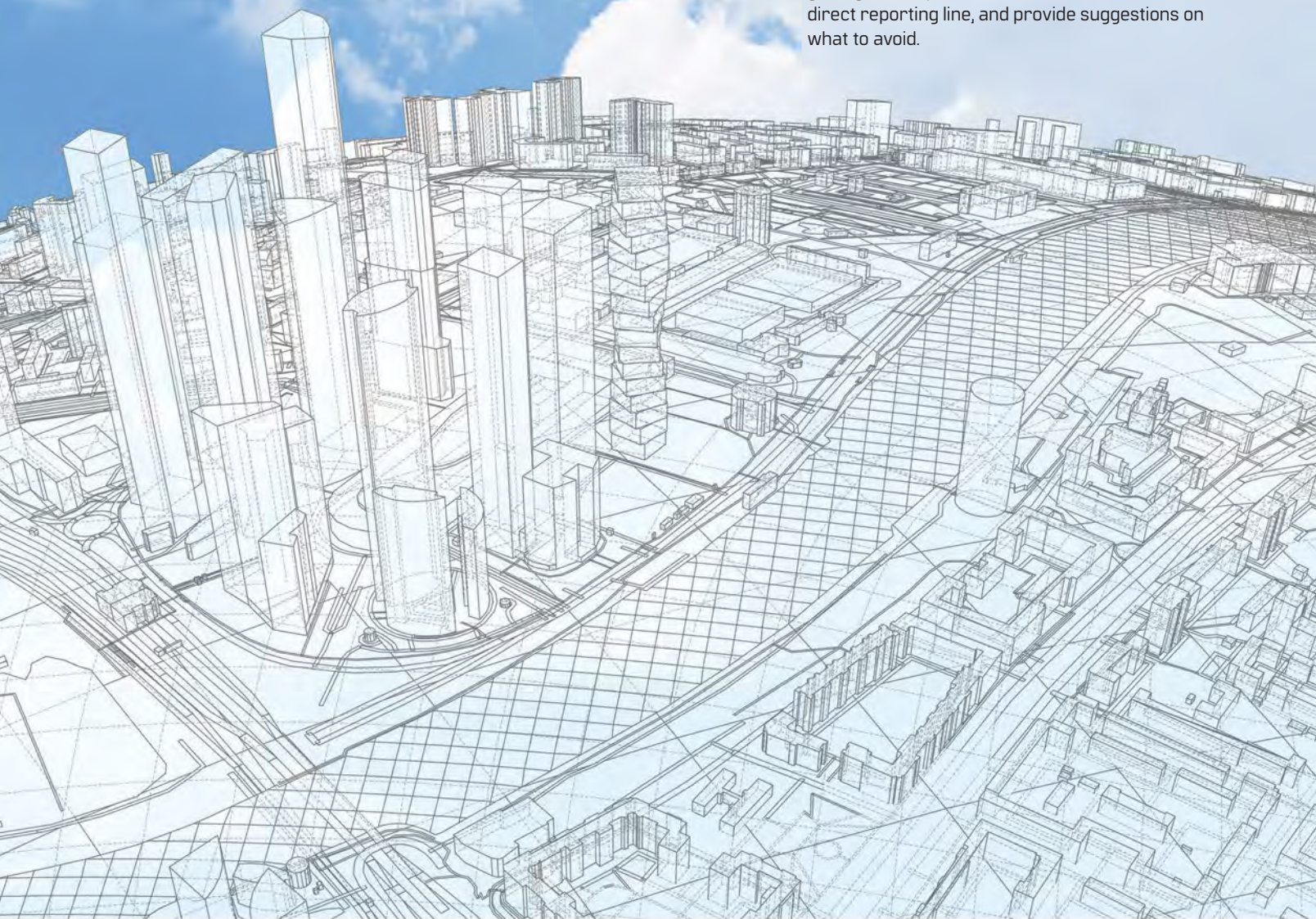
Sanjeev Menon, ACAMS Career Guidance columnist, compliance, legal and privacy senior practice area manager, Korn Ferry, New York, NY, USA, Sanjeev.Menon@KornFerry.com



MAKING THE LEAP TO MANAGEMENT

The world of anti-money laundering (AML) provides for many careers at all levels across many industries, including banking, financial technology (fintech), gaming, lending, insurance and many others. Career levels could include entry-level analysts, experienced investigators, team leads, supervisors, managers and department heads. Because the field of AML involves specialties such as program/governance, production (working alerts) and data science, there is room in the industry for every skill set imaginable. This creates the opportunity for an AML professional to progress from entry-level analyst to department head. Do not be surprised if that progression is not linear. Most of the time, that progress is not linear and instead involves spending time in at least two of the specialty areas above.

This article will explore the attributes of staff who are ready to be promoted, provide some tips for getting visibility for their attributes outside their direct reporting line, and provide suggestions on what to avoid.



ATTRIBUTES

Many professional and personal attributes are indicative of good first-level AML people managers. However, the attributes listed below were singled out to be the most important in staff deemed to be most promotable to their first AML-related managerial role:

- Ability to communicate, both verbally and in writing:** This includes providing clear and concise direction to others and summarizing and presenting information to all levels of the organization, including executive management and the board.
Examples: Training new AML alert investigators, explaining to the board the increased importance of sanctions, etc.
- Possession of a work ethic/get-it-done mentality:** This includes those who think outside of the box to get the job done, volunteer for projects and say "yes" to whatever needs to be done at the time, regardless of their title.
Example: An AML officer rolling up the sleeves to work on a country risk assessment to cover for someone on leave.
- Ability to identify and resolves issues:** This includes being inquisitive, thoughtful and constantly suggesting and striving toward solutions.
Example: A professional using the institution's existing staff for a customer due diligence lookback.
- Readiness to support staff members and their development:** This includes compassion, the ability to relate to staff, provide support, de-stress and build confidence. In general, this is a teammate who empowers others.
Example: A professional supporting staff obtaining the CAMS credential.
- Knowledge of being process-oriented and innovative:** This includes understanding processes, efficiencies, root-cause analysis, striving toward automation, staying current on how the industry is innovating and understanding the cause and effect of courses of action.
Example: A professional volunteering to be a test case for an artificial intelligence solution.
- Willingness to embrace continuous improvement:** This includes seeking feedback, building relationships and being willing to take risks in order to move forward.
Example: A professional embracing 360 reviews.
- Decisiveness:** This includes having confidence in one's abilities and avoiding "analysis paralysis."
Example: A professional seeks input but decides upon a new AML software in time to allow for a reasonable implementation plan.
- Knowledge of AML/counter-terrorist financing (CTF)/sanctions concepts:** This includes one's subject-matter expertise, and what is notable about this item is how low on the list it resides. Understanding AML/CTF/sanctions is important, but when one becomes a manager for the first time, the attributes appearing above on this list are likely more important.
Example: A professional allocating an hour of time per day to stay current on AML issues.
- Strategic thinking:** This includes being able to visualize goals and objectives; create and lead a plan; and maximize the resources available to execute strategies. Newly promoted managers need to develop this ability. For senior and executive managers, this attribute would be higher on the list.
Example: Understanding when the disruption of implementing new AML software is overshadowed by the benefits of that implementation.
- Trustworthiness/integrity:** No list of managerial attributes would be complete without this attribute being identified.
Example: Self-identifying a process weakness in the AML department to avoid regulatory action.

While it is great to have the right personal attributes that make one promotable, it is also important to make those attributes visible to the decision-makers in the organization





GETTING VISIBILITY

While it is great to have the right personal attributes that make one promotable, it is also important to make those attributes visible to the decision-makers in the organization. Every organization is different due to size and industry, but there are some general tips one can follow to display candidates' managerial attributes and hopefully increase the chance of being promoted to their first AML managerial role.

General tips:

- Keep an open mind and be a sponge:** If a role becomes available with greater responsibility, give consideration to it, even if it is not in your specialty. This will only help you rise to a department head if that type of position ever becomes available.
- Communicate:** Ensure that your supervisors are aware of your career aspirations toward a managerial role.
- Seek training:** Seek out management—and leadership—development programs in your organization.
- Showcase teamwork:** Seek out projects in your organization, whether AML-oriented or otherwise. These can highlight your teamwork skills and ability to manage people toward a common goal.
- Seek exposure:** Seek out committees and initiatives in your organization, such as a “Green Team” or the “Process Improvement Team,” as these provide exposure within the organization.
- Be engaged:** In all things you do in the organization, take an active role, ask questions, offer insights and engage with peers, as you never know who is watching. Consider all actions with managers and senior leaders as part of an observational interview process.

AML-related tips:

- Participate in AML industry groups:** Seek out leadership roles in industry groups. For example, a local ACAMS chapter may need AML professionals to organize a learning event or webinar or you could even join the board.
- Pursue AML professional development:** Educate yourself on what level of education and certifications your organization, or similar organizations, require for managerial roles, and pursue them. Continue enhancing your subject-matter expertise.
- Seek out an AML mentor:** The mentor can be part of your organization or an industry specialist.
- Create AML content:** You can publish articles, speak on webinars, create content for an internal or external newsletter, be a podcast guest, etc.

Most of the above tips are part of developing one's personal brand, and most begin with “seek” or a similar word because building a personal brand and obtaining visibility is an active sport; it takes effort. Did you notice that enhancing subject-matter expertise is the lowest on the list related to AML professional development? This is because becoming a better analyst might not equate with becoming a better manager. However, subject-matter competency is still required so that you can provide guidance and direction to direct reports and make informed decisions.

PITFALLS TO AVOID

if being promoted to a managerial-level position is one's goal:

- Staying in a comfort zone:** Seldom do promotions occur from comfort zones. Staying within one specialty can result in advancing to a point where a manager-level position is, in reality, a lower position. An example of this in many instances is that an analyst III might actually have a higher salary than an entry-level manager.
- Isolation:** Doing a great job but not developing the skills to interact with others in the organization, peer groups and industry organizations will hinder one's ability to see the bigger picture and be strategic.
- Failure to have a plan:** If one's goal on Monday is to move forward with AML systems and data, but on Tuesday it is to move forward with AML investigations, and on Wednesday it is to focus on AML program/governance, the rapid and constant changing of focus will harm your career in general. This is not to say that once you have developed a certain mastery in one area, you should not move to another area. You actually should. But it takes time to master an area.
- Constant perfection:** There are times when something has to be perfect, such as AML data mapping, but for most AML practitioners, the goal should not be perfection. There is no expectation of having a perfectly worked alert, a perfectly written suspicious activity report or a perfectly written enhanced due diligence report. Constantly striving for perfection could thwart one's ability to see the bigger picture.
- Conveying a negative attitude:** It is OK to challenge, but constantly conveying negative messaging could dampen one's chances at promotion.
- Failure to convey confidence:** It is possible to convey confidence without seeming boorish. It is important to find that balance.
- Failure to navigate politics:** All organizations have some level of politics going on. Learn to steer clear of land mines.
- Conveying an attitude of entitlement:** This could leave the impression to management that one is not willing to work hard for something.
- Misperceiving years of experience:** Understand the difference between having 10 years of experience in AML versus having one year of experience in AML 10 times over, meaning doing the same exact thing for 10 years.
- Failure to be a self-starter, self-learner, etc.:** Many of the skills, attributes and knowledge needed to be promoted require a lot of extra effort.

Conclusion

For some AML professionals, getting that first promotion to management is a professional and personal goal, and most AML departments provide numerous avenues for a managerial career path. The advice above should help provide strategies—both AML-focused and in general—to AML professionals who seek their first managerial role. **AT**

Sharon A. Blanchette, CAMS, Compliance Audit Control manager and advisor, Cenlar FSB, Yardley, PA, sablanchette@cenlar.com

Contributors:

Amy Wotapka, CAMS, BSA and OFAC officer, First American Bank, Kenosha, WI, awotapka@firstambank.com

Larry Gordon, CAMS, managing director, Gordon Risk Solutions, Columbus, OH, larry.gordon@gordonrisk.com

Mario Duron, CAMS, global head of Crypto Compliance, Chipper Cash, San Francisco, CA, mario@chippercash.com

Vernon Tanner, CAMS, vice president, AML/BSA officer, 1st Franklin Financial Corporation, Toccoa, GA, vtanner@1FFC.com

Bart Mierzejewski, CAMS, director, Global Compliance Operations, Uphold, Inc., New York, NY, bart.mierzejewski@uphold.com

Juliana Bogatinoska, CAMS, BSA officer, OceanFirst Bank, Toms River, NJ, jbogatinoska@oceanfirst.com



Lash Kaur:

Bettering the world through social impact



ACAMS' Vice President of Global Strategic Communications and Diversity, Equity and Inclusion (DEI) Lash Kaur spoke to *ACAMS Today* about her responsibility for leading the organization's stakeholder relations, which includes employee and external communications, all social impact initiatives and advisory board relations, and is newly responsible for ACAMS' environmental, social and governance (ESG) strategic planning and reporting. In addition, Kaur oversees the organization's expansive global chapter network.

Kaur joined ACAMS in January 2019 as she was drawn to the remarkable social impact opportunities at ACAMS and the role presented, most notably, playing a role in fighting modern-day slavery and human trafficking (HT). Through her work and the robust cross-functional partnerships Kaur and her team have created, she works intentionally to elevate ACAMS' world-class expertise, thought leadership and global positioning, all in an effort to initiate deep, meaningful and measurable change in the world of financial crime prevention.

Prior to joining ACAMS, Kaur was the regional head of communications for Laureate Education, Inc., a NASDAQ-listed education company. In her capacity as vice president of communications for the European, Middle Eastern, African and Asian (EMEAA) regions, she drove brand building, change management and social impact initiatives across the region.

ACAMS Today (AT): What drew you to ACAMS? What was it about the organization that inspired your interest?

Lash Kaur (LK): I have always been drawn to mission-driven roles and spent the decade prior to ACAMS in the education space, where we offered opportunities to students in countries where education was often a privilege and not a right. I was tapped for the role at ACAMS in the fall of 2018, and I did not need much persuasion, as I was immediately drawn to the mission. The thought of joining an organization that could drive deep and measurable change in the world was impossible to resist.

AT: What does a typical workday look like for you?

LK: To be frank, no two days are the same, as my role covers a range of responsibilities. I may start my day discussing a new scholarship or a mentorship initiative for Black, Indigenous and people of color, move on to discussing press release angles and end it with a meeting to discuss an interview with the Financial Action Task Force president. The thread that ties everything together is our mission, but every day consists of me and my team furthering our relationships across the organization, establishing new partnerships or opportunities that can advance brand awareness, enrich engagement and ultimately further the impact we can have in the world.

AT: What aspect of your job do you enjoy the most?

LK: I think “mission-driven” is quite an overplayed term (in general), but what I love most about my role and ACAMS is that it is unequivocally true here. As a communications practitioner, authenticity is key. And through my role here at ACAMS, I know that we can show up every day and truly, authentically be who we are, what we say we are—and with impactful, industry-leading results. We are so steadfast in our mission to fight financial crime and ultimately aid in stopping the subsequent harm that financial crimes fund, such as

modern-day slavery, HT and illegal wildlife trade. Being at the epicenter of this commitment motivates, inspires and really excites me every single day.

AT: How did your prior experience with Laureate Education, Inc., your own communications company and working as a journalist prepare you for your role at ACAMS?

LK: During my time at Laureate, my experiences varied so much that it was almost surreal. I coordinated visits by former global leaders such as President Bill Clinton and British Prime Minister Tony Blair, and in parallel mentored and partnered students from the most impoverished communities and worked on sustainability projects with female inmates in one of the largest prison complexes in South Asia. The time with Laureate has helped me tremendously in my current role, as I had deep operational experience and learned to work across geographies. I saw the power of stakeholder engagement and I love having the ability to engage key stakeholders to be a driving force in my current role. My prior roles also rooted me in the world of social impact. The ability to drive measurable and long-term impact that could be shared with the world through data storytelling meant that I was often a change agent.

AT: What changes have you seen at ACAMS since you joined in 2019?

LK: ACAMS has evolved tremendously since I joined. We are much more focused on our mission, our community, and our ability to educate, inform and convene. For instance, we have launched five free social impact certificates since 2020 that strive to end HT,¹ modern slavery,² illegal wildlife trade³ and online child exploitation.⁴ Of those certificates, there have been more than 40,000 enrollments that span more than 100 countries to date. We continue to innovate and provide solutions for the world's most pressing issues and that is very meaningful to be part of and lead! We have an incredibly impressive, thoughtful, world-class thought leadership team that provides guidance and resources on the

most critical issues in a timely manner. We have an engaged global community that stayed together during the darkest days of the global pandemic. The ACAMS team continues to grow in strength (and force) each day and we have a great leadership team. While a lot has changed over the years, one element that I believe is very special to our organization is that the people are good, the people are passionate and dedicated; it creates our “soul” per se, and the energy is inspiring, impactful and I know it will deliver more good in the world. From a personal standpoint, being a woman of color from Asia, I love and celebrate the opportunity to be recognized for my abilities, achievements and the fantastic relationships I have developed across the organization.

AT: What do you like to do when you are off the clock?

LK: I am like a plant that needs the sun and fresh air to thrive! Being outdoors invigorates me and I love nature treks and hikes. I also mentor young people who keep me on my toes and challenge me on a regular basis. And when I really want to unwind and disconnect, I pick up a book and turn to my favorite playlist on Spotify! **AT**

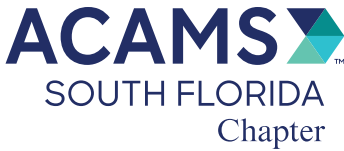
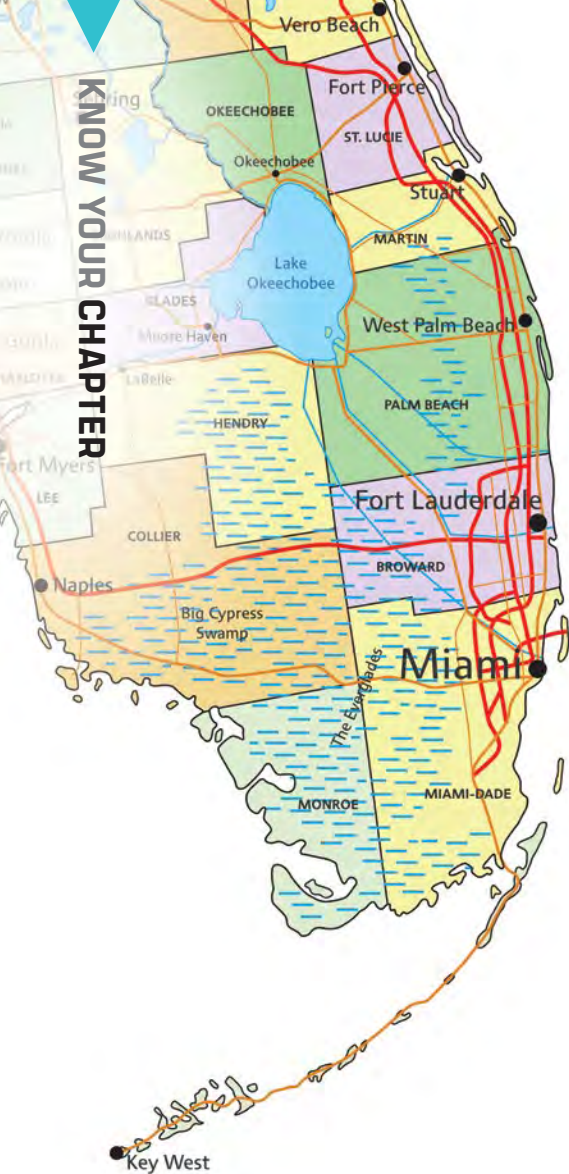
Interviewed by: ACAMS Today editorial, ACAMS, editor@acams.org

¹ For more information about ACAMS' Fighting Modern Slavery and Human Trafficking Part 1 certificate, please visit: <https://www.acams.org/en/training/certificates/fighting-modern-slavery-and-human-trafficking/>; For more information about ACAMS' Fighting Modern Slavery and Human Trafficking Part 2: U.S. Sex & Exploitation Cases certificate, please visit: <https://www.acams.org/en/training/certificates/fighting-modern-slavery-and-human-trafficking-part-2>

² Ibid.

³ For more information about ACAMS' Ending Illegal Wildlife Trade—A Comprehensive Overview certificate, please visit: <https://www.acams.org/en/training/certificates/ending-illegal-wildlife-trade/>; For more information about ACAMS' Ending Illegal Wildlife Trade—A Practical Guide for Law Enforcement, please visit: <https://www.acams.org/en/training/certificates/ending-illegal-wildlife-trade-a-practical-guide-for-law-enforcement>

⁴ For more information about ACAMS' Preventing Online Child Exploitation with Financial Intelligence: An Overview certificate, please visit: <https://www.acams.org/en/training/certificates/preventing-online-child-exploitation-with-financial-intelligence-an-overview#overview-e430ae7c>



Spotlight on the ACAMS South Florida Chapter

The last few years proved to be transformative for how and where we work. Pushed by the pandemic, many in the anti-financial crime (AFC) community moved into remote-only or hybrid work environments. Many in the AFC community also made a far greater leap and moved across the country to be closer to families and friends or simply to seek better weather, lower taxes and amazing beaches like those found in South Florida. This migration of AFC talent is one of the key drivers for a revitalized, reimagined and growing ACAMS South Florida Chapter. In the throes of the pandemic, countless AFC professionals—many from the greater New York City area—arrived in the Sunshine State and settled near Miami, Ft. Lauderdale and Palm Beach.

These moves did not just make sense for personal reasons—South Florida is not only an important international business and banking hub, but it is also a long-standing, global hub for financial crime. From drug money laundering to mortgage fraud and every type of financial crime in between, South Florida has long been a top spot for illicit financial activity. Our sophisticated financial sector, dynamic hospitality and

tourism business, and our status as a global trade, travel and logistical hub, are just a few of the factors that attract money launderers and fraudsters to our area. These factors also make South Florida a natural home for a vibrant community of financial crime fighters and trained professionals dedicated to protecting the best our communities have to offer.

Filled with passion for continuing and enhancing their AFC education, these transplants have begun to join the ACAMS South Florida Chapter's ranks. Like other global ACAMS chapters, the South Florida Chapter reignited operations in 2022 and focused on offering free webinars for our members. Last year, the chapter hosted six webinars centered on top and emerging risks such as Russia sanctions threats in the region, elder financial exploitation, the abuse of economic citizenship programs by corrupt actors and criminal networks, the use of cryptocurrencies for money laundering purposes, human trafficking and modern slavery, as well as the growth of environmental crimes—such as illegal mining, illegal logging and the illegal wildlife trade—to generate criminal revenues. The chapter hosted excellent speakers from across the U.S. government, including the U.S. Department of the Treasury, as well as innovative technology companies and leading nonprofit organizations.

2023 chapter programming

In 2023, the chapter is focusing efforts on more in-person events that will bring AFC professionals back together face-to-face to learn about the top and emerging risks and best practices, as well as to build relationships. The kick-off in-person event will be held in March and this will be the chapter's first-ever U.S. law enforcement (LE) roundtable. The chapter hopes to bring 2022's success in the virtual domain to more interactive settings and provide new opportunities for AFC professionals from across the public and private sectors to engage in meaningful

ways. The chapter's goals include enabling dialogue and information sharing, educating members and inspiring the next generation of AFC professionals through partnerships with local universities.

The 2023 chapter programming will offer a mix of virtual and in-person events across the South Florida area (i.e., Miami-Dade, Broward and Palm Beach counties). In January, for example, for our first virtual event of the year, we hosted Claudia Helms from the Washington, D.C.-based nonprofit Global Financial Integrity (GFI). Helms discussed illicit financial risks stemming from digital assets, how governments across Latin America and the Caribbean are developing their respective regulatory frameworks and GFI's data-driven analysis. In February, we hosted another Washington, D.C.-based, innovative nonprofit organization, the Center for Advanced Defense Studies (C4ADS), as well as the World Wildlife Fund (WWF), to discuss the illegal wildlife trade, related illicit financial activity and how financial institutions can work more closely with nonprofits to share knowledge and proactively mitigate financial crime risks.

For the aforementioned March U.S. LE roundtable, audience members will hear about the top and emerging illicit financial trends and case studies from South Florida LE leaders. They will also learn about the best ways to share information and partner with LE partners.


New chapter leadership

In 2022, the chapter welcomed several new board members with extensive and wide-ranging industry experience. These new members bring unique experience, energy and dynamism to the fight against financial crime in South Florida.

- Alek Dvoskin (PayPal) recently moved to South Florida and joined our leadership ranks from the ACAMS Phoenix Chapter, where he oversaw programming and helped the chapter grow significantly in recent years. He offers deep experience in international banking, financial technology (fintech) and the U.S. LE world.
- Jocelyn Baez (Cross River) joined the board and lends an important international banking and fintech perspective to the chapter's efforts. Before joining Cross River as an FCC Program project manager, she spent six years with HSBC and is a graduate of both Florida International University (FIU) and the University of Florida (UF).
- Alex Egan joined us from Kaufman Rossin, oversees membership engagement, and was recently profiled in an *ACAMS Today* article, which featured his LE and U.S. Army experience. Prior to joining Kaufman Rossin, he was an associate principal with the Financial Industry Regulatory Authority (FINRA) and a former criminal investigator assigned to the Federal Bureau of Investigation's Fraud Task Force. Among several degrees, Egan earned a Master of Accounting from the University of Miami.
- New board co-chair Nick Schumann (HSBC) also joined the board in 2022 and brought AFC experience from both his U.S. Department of the Treasury and U.S. Army roles. In the fall of 2022, he authored an article for *ACAMS Today* on the value that military veterans bring to the AFC community and is heavily involved in local and national efforts to support veterans in their transition to the financial services industry. Like, Baez, he is a proud alum of both UF and FIU.
- Jay Fisher, formerly a sanctions investigator with the Office of Foreign Assets Control (OFAC), joined us in 2022 from USAA and lent the chapter his experience in the sanctions arena. Before joining USAA, he served as the U.S. Department of the Treasury's senior advisor to U.S. Southern Command (SOUTHCOM) on illicit finance issues in Latin America and the Caribbean.
- Dan Wager joined us from PwC and brings tremendous experience from his time in U.S. LE, banking and consulting, as well as his prior role helping to build out the ACAMS New York Chapter.
- Lastly, also though not a new board member, it is worth noting that Sissy Oliver-Adams (Protiviti) was profiled in *ACAMS Today* and by the University of Florida in 2022 for her many contributions to the AFC community.

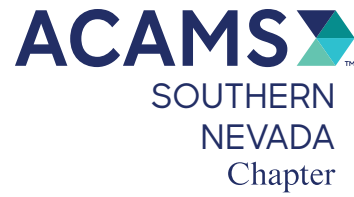
During the March roundtable, we will honor the important contributions of recently departed board members during an awards ceremony and highlight their efforts to strengthen our local financial crime-fighting community over the years. Thankfully, the board enjoys continuity with the guidance and experience provided by other board members like Brian Frankel (co-chair) and Jeferson Moreira (treasurer).

Conclusion

This is an exciting and unique time to be a member of the AFC community. It is not necessarily an easy time, but our jobs certainly are not boring. New challenges regularly emerge, especially if you work in South Florida. As we know, money launderers and fraudsters never stop innovating or developing schemes to skirt laws and evade scrutiny. Our work as financial crime fighters, therefore, is more important than ever. And one could argue that South Florida is ground zero for this fight. If you recently moved to South Florida or are slowly masterminding your professional escape to the Sunshine State, rest assured that the ACAMS South Florida Chapter will help address your AFC educational needs. Come join the fight and please consider joining our ranks. We need you and your contributions to be the best chapter we can be and further build and strengthen our vibrant community of financial crime fighters. 

Alek Dvoskin, CAMS, chapter head of Programming, LinkedIn

Nick Schumann, chapter co-chair, CAMS, U.S. head of Financial Crime Program, Framework, and Engagement, HSBC USA, LinkedIn



Location, location, location and 2022 in review

ACAMS Southern Nevada Chapter is happy to call Las Vegas its home. The city is an internationally renowned major resort destination known primarily for its entertainment, fine dining, gambling, shopping and nightlife. Las Vegas is among the top destinations in the U.S. for business travel, holding over 22,000 conventions of different sizes every year. It also ranks as one of the world's most visited tourist destinations, attracting over 40 million visitors each year. In addition, the city became a sports destination after welcoming major professional teams like the Vegas Golden Knights, the Las Vegas Raiders and the Aces.

Whatever may be the reason for visiting Las Vegas, there is a multitude of things to do, see or learn here. A trip to the area can change one's life, whether they become a millionaire overnight or lose their entire life savings. Here is a fun fact—the largest slot jackpot in history worth \$39.7 million was won 20 years ago at the Excalibur Casino in Las Vegas.¹ A \$100 bill can transform your life; just do not let that last \$100 bill get swallowed by a Megabucks slot machine.

Las Vegas has quite a history and there are great features that make this city a treasure trove for any anti-money laundering (AML) compliance guru. Its past is best described in the halls of the Mob Museum, which is dedicated to the tumultuous relationship between organized crime and law enforcement (LE) in Las Vegas and the entire U.S. Visitors can

watch a film about the history of organized crime, learn about mob violence, illegal gambling or travel back in time to the 1920s era of the Prohibition by visiting the museum's underground speakeasy and distillery.

When mobsters started flocking to Las Vegas in the early 1930s, this brought criminal activity to the area, such as prostitution and other illegal businesses that started to develop here. With the availability of adult entertainment and due to soaring crime rates of the last century, Las Vegas earned its notorious nickname as "Sin City." While this was in the past, and Nevada remains the only state in the U.S. where legal prostitution exists, prostitution is illegal in Las Vegas and the wider Clark County.

To add to its Sin City name, Nevada is a state that has licensed both medical and recreational marijuana dispensaries. Back in 2000, Nevada voted to legalize medicinal marijuana, and in 2016, adult-use cannabis was permitted. Today, anyone 21 years or older can legally purchase cannabis in Las Vegas. Based on the Controlled Substances Act of 1970, the possession and use of cannabis are illegal under federal law in the U.S., thus giving plenty of topics for discussions for the AML community not just in Las Vegas but around the country.

With its importance as a convention and tourist destination, and due to its history, it only makes sense that every year, in the fall, ACAMS hosts its *ACAMS Annual AML and Financial Crime Conference* (this year its 22nd) in Las Vegas. Attendees gather to hear from regulators, LE and experts on trending topics, such as AML, anti-fraud or anti-corruption and compliance.





ACAMS Southern Nevada Chapter members mixing at the chapter's social event on June 16.

The mission of the ACAMS Southern Nevada Chapter is to support the goals of the ACAMS organization in providing outstanding learning and professional development opportunities, as well as support its members' needs in the AML community. The chapter strives to fulfill its mission by providing high-quality meetings, workshops and networking events where members and nonmembers can build knowledge related to compliance, enhance their skills and share experiences.

A look back at the chapter's 2022 activities

June 2022: Social event

After a period of remote meetings, the chapter's social event had a great turnout. The board members were introduced to the compliance community in Las Vegas, details were highlighted about the benefits of ACAMS membership and a description of future educational events was announced. The chapter had seen a more diversified audience this time, including folks from the gaming, auditing, consulting, crypto and banking industries, as well as representatives from the Las Vegas Drug Enforcement Administration office.

August 2022: Human trafficking (HT) event

The chapter hosted the first event of a two-part series focusing on the measures to mitigate the risks of HT in and around Las Vegas, which is one of the most critical issues in the area. Elynn Greene, who serves as the manager of Victim Services and Human Trafficking at the Las Vegas Metropolitan Police Department, highlighted the red flag indicators and described the challenges we are facing as a community, as well as the resources available to HT victims in Southern Nevada. The Las Vegas Metropolitan Police Department Gangs/Vice Bureau provided additional resources, statistics as well as warning signs that help recognize prostitution and HT.

October 2022: HT webinar

To continue the discussion about HT, the webinar on HT typologies, red flags and investigative techniques became one of the most attended events organized by the chapter. Participants enjoyed the event and asked lots of questions during the webinar, where Larry Cameron from the Anti-Human Trafficking Intelligence Initiative presented various methods for implementing anti-HT programs at financial institutions, crypto businesses and casinos. The speaker also went over compliance integration, data sets and typologies, as well as open-source intelligence and investigative techniques.

December 2022: Digital payments event

The last event of the year focused on the ever-growing digital payments industry as the world becomes increasingly digital. The event presenters included Senior Vice President of Business Development at Sightline Payments Tamara Tenenbaum, BetMGM's Chief Compliance Officer Rhea Loney, and Managing Director at Eilers & Krejcik Gaming Payments Jerry Rau, who covered the current regulatory landscape, AML and fraud trends. The panel provided attendees with insights both in theory and in practice about important issues, red flags, trends to be aware of and ways to navigate the digital payments landscape.

The speaker, Elynn Greene, giving a presentation on mitigating human trafficking risks at the ACAMS Southern Nevada Chapter Human Trafficking Training on August 31.





Pictured from left to right are ACAMS Southern Nevada Chapter Board Members: Maria Guzman, Alistair Cameron, Tudor Prisneac, Nick Langenfeld, Kim Barley, Sean Topchi and Jessica Griffith.

2023 looks promising

We conducted a survey where 60% of responders voted for a future mix of in-person and virtual events; 30% wanted to learn more about the Anti-Money Laundering Act of 2020, while 25% were interested in learning about customer onboarding and know your customer (KYC) and 15% about iGaming and sports betting topics. Based on the results, our target audience represents 40% coming from the gaming industry while 30% are AML specialists with a financial services background.

To begin on the right note, and since over 80% of our survey responders wanted another AML networking event, compliance experts met at our first social event of 2023 on March 2. Specialists in banking, gaming, financial technology and LE learned about upcoming 2023 events and chapter membership benefits, and created new connections with others in the field.

Another exciting upcoming training session is planned for April 26 between 11:30 a.m. and 2 p.m. at the Sierra Gold, 6515 S. Jones Blvd., Las Vegas, NV 89118. Event sponsor and presenters from Thomson Reuters will discuss synthetic identity fraud and the KYC and know your business topic. Compliance professionals will learn about the current types of identity fraud; how fraudsters have adapted to pandemic changes; identify some of the challenges in detecting and stopping fraud; and how a proactive approach can mitigate those challenges. Lastly,

participants will learn how identity verification tools are integrated into compliance standard workflows, improving risk management and giving folks better visibility into their customers.

As the chapter events provide a good landscape to meet experts in the AML community, our focus is to prevent money laundering and keep our communities safe. We will continue to work together toward educating our compliance followers, and we look forward to seeing everyone at our future educational events, with more dates being announced soon!² AT

ACAMS Southern Nevada Chapter Board,
sonevada.acams@gmail.com

¹ "World Record Slot Jackpot Hits at Excalibur in Las Vegas," *IGT*, March 21, 2003, <https://irigt.com/news/news-details/2003/World-Record-Slot-Jackpot-Hits-at-Excalibur-in-Las-Vegas/default.aspx>

² For the exact date, time and location of the upcoming events, join the ACAMS Southern Nevada Chapter's LinkedIn group: <https://www.linkedin.com/groups/6715766/> or follow the chapter's ACAMS page: <https://www.acams.org/en/chapters/united-states-west/southern-nevada-chapter>.



The launch of the ACAMS Italy Chapter and what comes ahead!



The ACAMS Italy Chapter's event in November, which marked the chapter's launch, featured a roundtable discussion with (left to right) moderator Angelo Mincuzzi of *Il Sole 24 Ore*, Nico di Gabriele of European Central Bank, Arianna Rovetto of Banco BPM Group, Marco Pacino of the Bank of Italy and Sabrina Galmarini of Annunziata & Conso.



On November 21, 2022, the ACAMS Italy Chapter hosted its first in-person event in Milano for the chapter's launch, making the Italy Chapter the 62nd chapter worldwide and 15th in Europe.

Marking its first meeting at the glamorous Excelsior Hotel Gallia, the newly formed Italy Chapter brought together a team of anti-money laundering (AML) and anti-financial crime (AFC) and compliance professionals with solid and complementary backgrounds.

Presenting the board, Michele Valeriani, global head of anti-financial crime compliance at Assicurazioni Generali Group Generali, highlighted that diversity is the key driver that connects the seven board members in terms of their roles, gender and experience, considering the added value brought by the members' different backgrounds as a main strength. The board includes Sabrina Emilia di Feo, internal audit senior manager, UniCredit Group Holding; Arianna Rovetto, group head of AML at Banco BPM; Michele Valeriani, global head of anti-financial crime compliance for Generali and member of the Group Risk and Control Committee;

Alberto Armani, senior director, group head of KYC-AML at Intesa Sanpaolo; Marco Valcavi, AML officer/money laundering reporting officer at Flowe S.p.A., Mediolanum Fiduciaria S.p.A. and Prexta S.p.A.; Nicola Passariello, director and financial crime practice lead for Europe and Africa at Moody's Analytics; and Francesco Monini, managing director and FSI Audit & Compliance Italy Practice Leader at Protiviti.

Created and run by the above-mentioned team of local AFC professionals, the ACAMS Italy Chapter is an important part of the ACAMS community. According to its mission statement, it plans to:

- Provide a platform for continuous development and networking among AFC and sanctions professionals in Italy.
- Bring relevant content to the AFC community by sharing knowledge and expertise through regular meetings and events held in both English and Italian.

- Facilitate an open dialogue across the AFC crime community between governments, regulators, law enforcement and supervised entities to develop a solid partnership for managing money laundering, terrorist financing and sanctions-related risks.
- Focus on augmenting ACAMS' overall AFC education and training efforts.

In the context of this challenging mission and reflecting the driver of diversity, the chapter hosted its launch event in November—a seminar at the Excelsior Hotel Gallia—that drew over 120 AFC professionals from many different industries and sectors. Attendees included personnel from global banking and insurance institutions, money services businesses (MSBs) and development banks, as well as AML professionals, forensic and risk management experts, police officers and members of public authorities.

The successful evening event featured presentations from notable guests and panel discussions, as well as a network reception. Moderated by Angelo Mincuzzi, a special correspondent for *Il Sole 24 Ore*, the seminar included a keynote address by Blake Pritchett, deputy director of the U.S. Department of State's Office of Economic Sanctions Policy and Implementation. The roundtable discussion featured Nico di Gabriele, senior team leader for European Central Bank; Marco Pacini, manager at the Bank of Italy's Inspectorate Department;¹ Arianna Rovetto, group head of AML at Banco BPM Group; and Sabrina Galmarini, counsel at Annunziata & Conso.

The panelists shared their views on AML/counter-terrorist financing (CTF) topics, including the relationship between prevention and enforcement of financial crime, the use of new technologies by criminals to commit crimes, what AFC professionals are doing to combat financial crimes, the role

Pictured from left to right are Alice Bufalini, Yi Lin Koo, Mariah Gause, Paola Santini, George Voloshin, Lashvinder Kaur and Monica Blaj.





ACAMS Italy Chapter launch event attendees enjoying refreshments.

of knowledge in understanding how AML operates, and building better and more insightful public-private partnerships for the sake of better cooperation and also with AML supervisors.

To build on the enthusiastic interest in the launch event, the ACAMS Italy Chapter board plans to continue professional development and education events throughout the year. These initiatives, which will be announced and organized starting in the first quarter of 2023, include a seminar on new trends in combating financial crimes focused on technology innovation and peer collaboration and a specific training initiative on sanctions.

In addition, the chapter is looking forward to focusing on other key topics, including the beneficial ownership register; the upcoming version of the Bank of Italy's requirements regarding organization, procedures and controls that follow the European Banking Authority's guidelines; the new risk indicators from Italy's Financial Intelligence Unit; and the role of cryptocurrencies and crypto-assets in the AML framework.

This kind of ambitious program reflects the primary purpose of the ACAMS Italy Chapter, which is to foster the creation of a wide community of AML/CTF professionals, adding value to local ACAMS members, and providing a peer networking and educational forum for the furthering of best practices in AML and financial crime prevention and detection in Italy.

The launch of the new ACAMS Italy Chapter reflects the ambition of our country to play a key role in the AFC sector while promoting open dialogue among all AFC professionals in the public and private sectors and providing a venue for Italy's AFC professionals to share their experiences. **AT**

ACAMS Italy Chapter Board, acamsitalychapter@yahoo.com

¹ Marco Pacini's participation was on his own behalf.



ADVANCED CERTIFICATION GRADUATES: DECEMBER–FEBRUARY

Graduates' countries/regions are sorted alphabetically

Australia

Chi Kwan Kong, CAMS-Audit

Canada

Gabor Fekete, CAMS-Audit

Cayman Islands

Tingting Li, CAMS-Audit

Guam

Jacinta Benavente Elm, CAMS-RM

Haiti

Rose Bianca Jean Mary, CAMS-RM

Hong Kong

Chi Hang Esther Law, CAMS-RM

Indonesia

Laurentius Halimkesuma, CAMS-Audit

Kazakhstan

Valikhan Gusmanov, CAMS-Audit

Kenya

Hilda Kerubo Ondari, CAMS-RM

Luxembourg

Anne Cecile R. Plouhinec, CAMS-RM

Netherlands

Gregory Egbobawaye, CAMS-RM

Peru

Armando Martin G. Vasquez, CAMS-RM

Puerto Rico

Carla Matos Cabrera, CAMS-RM

Singapore

Jane Cheong, CAMS-RM

Suan Jin Anthony Foo, CAMS-RM

Hai Liang Gan, CAMS-Audit

Shirley Goh, CAMS-Audit

Mandy Huang, CAMS-Audit

Kian Sing Vincent Koh, CAMS-RM

Pak Nian Lam, CAMS-RM

Leon Xiang Feng Low, CAMS-Audit

Devonna Ng, CAMS-RM

Ying Fang Quek, CAMS-Audit

Wenxun Tay, CAMS-FCI

Solomon Islands

Kogulan Kaneshanathan, CAMS-Audit

South Africa

Oliver Jonathan Hill, CAMS-Audit

Switzerland

Cristina H. V. de Fleckenstein, CAMS-RM

United Arab Emirates

Senthil Prabhu Vasagan, CAMS-RM

United Kingdom

Nana Yaa Oheneasah, CAMS-RM

Petros Tryphonides, CAMS-FCI

United States

Janet Lee Cornett, CAMS-FCI

Dawn E. Davidson, CAMS-Audit

Carolyn Dicharry, CAMS-Audit

Christopher Green, CAMS-Audit

Tiffany Chevon Jones, CAMS-FCI

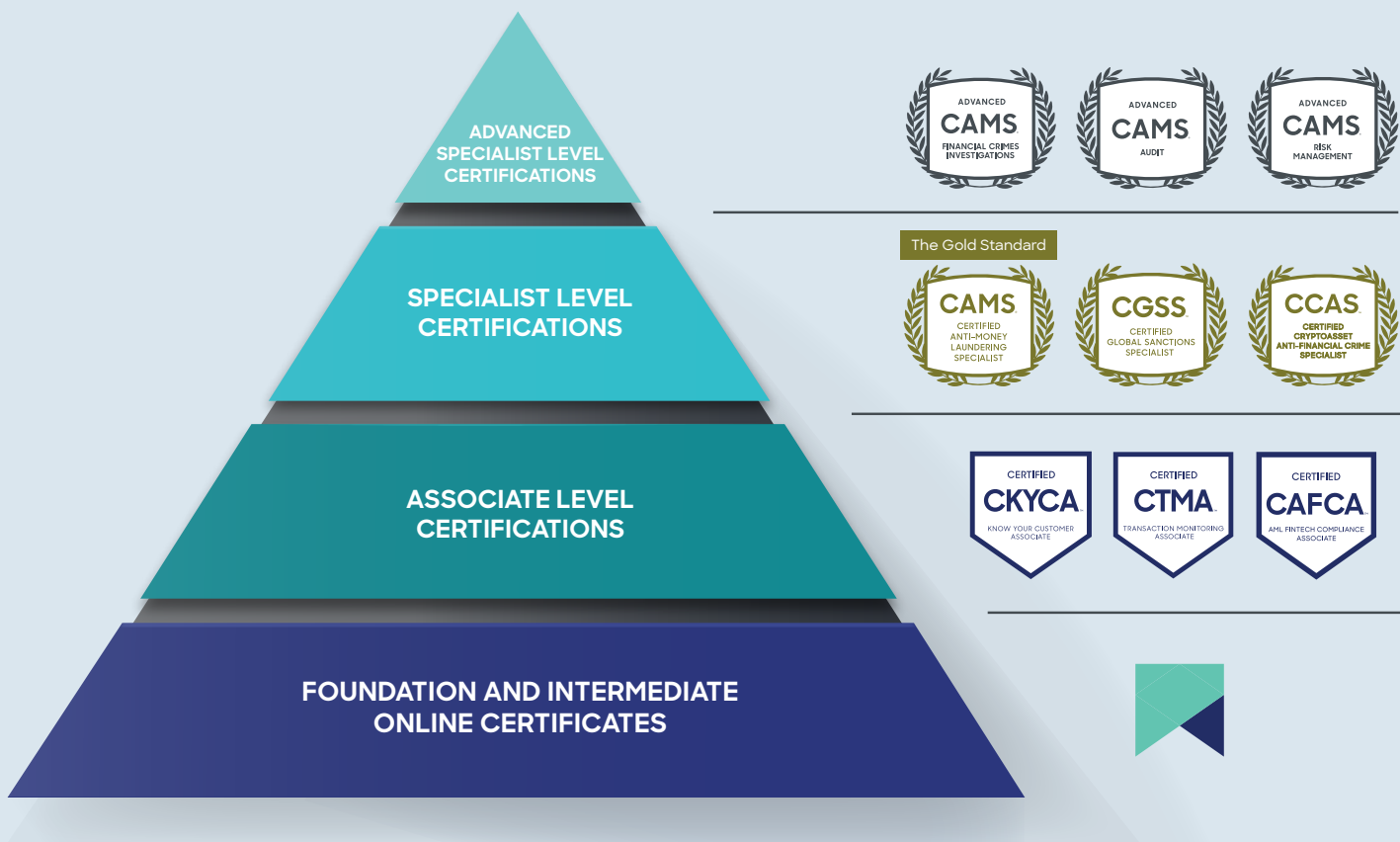
Carol Setterstrom, CAMS-FCI



TAILORED TRAINING SOLUTIONS

Our world-class training and accreditation programs help global organizations stay ahead of financial crime - now and in the future.

www.acams.org





CAMS GRADUATES: DECEMBER–FEBRUARY

Graduates' countries/regions are sorted alphabetically

Afghanistan

Hisashi Hokiyama
Mustafa Rasooli

Albania

Edval Zoto

Antigua and Barbuda

Rosemary Mannix

Armenia

Hermine Jumayan

Australia

Muhammad Basim Awan
Mahesh Balakrishnan
Karen Brohier
Paula Draney
Salome Hallock
Anandan Narayan Kaimal
Uthpala Kariyapperuma
Sarita Kumari Kashyap
Steve Dong Joon Kim
Michael Krawczyk
Matthew Brian Leadbetter
Da Li
Meng Li
Xiao Li
Angeline Mahwendepi
Yogesh Maini
Ana Maric
Clifford Scott Mells
Vindya Nadugala Mohottige
Mandy Mun Theng Ng
Peter Duc Hung Nguyen
Robert Edward Oliver
David Pilipovic
Timothy Elliot Pont
Sarah Robson
Yan Rui

Han Shi
Ankeeta Shrestha
Sun Zhu
Zen Taureka
Swathi Thamban
Song Hao Wang
Ruben Whyte
Xue Yuming

Austria

Gregor Auburger
Zijia Cong

Azerbaijan

Kamala Azimova

Bahamas

Sasha Natovia Alise Albury
Ianna Bethel
Mekel R. Bowe
Shanika Johnson
Yasmin Ariana Morris
Patricia Roberts
Selena Sawyer
Allistaire Stubbs
Gary Wilson

Bahrain

Ali Alaswad
Fatema Almadhi
Mohamed Als Salman
Chitrang Rathod
Amal Safar
Vyshak Sasidharan
Satya Srinivas Ventrpragada

Bangladesh

Tamanna Habib
Md. Abdul Halim
Md. Mamun Hasan
Muhammad Nazmul Hasan

Barbados

Estherline O'Neal

Belgium

Stephane Godde
Deepesh Narain
Louison Neuville

Bermuda

Quaejah Lateece Cox
Keisha Deniese Ramsay
Steven Keith Skinner

Brazil

Julia de Oliveira

British Virgin Islands

Giselle Jackman Lumy
Nada Y. Marrugo

Brunei

Kok Kiong Chong

Bulgaria

Mihail Hristov
Hannah Kang

Cambodia

Nitin Damodaran
Bolin Pheang
Kosal Uk

Cameroon

Gaëtan Nzali Wega

Canada

Cole Abbott
Temitope Adegun
Omotosho Folorunso Ajibade

Jeanette Au
Nadra Benchikh Lefgoun
Sean Boulton
Shu Chen
Nathalie Cormier
Lina D'Abramo
David Michael Danelutti
Rajendran Dhanasekharan
Sampath Ekanayake
Nora Eze
Esther Po Man Fan
Shivam Garg
Beatrice E. Hane
Shiloh Heckman
Mitchell Hirshhorn
Daniel Jensen
Elango Kalimuthu
Kihyu Kim
Frederic Lapalme
Danica Law
David Jihyung Lee
Ningjie Lu
Vanessa Clare MacKenzie
Fiona Madden
Lakshmi Manikandan
Erick Martinez
Daniel Matsinhe
Karelyn Murray
Muhammad Nouman
Ayoyinka Ogbé
Adetoke Ogunmoyela
Ayobami Ogunmoyin
Yemissi Nathalie Omiyale
Mariam Ololade Omotosho
Ewere Stephanie Omumu
Thi Nam Tran Pham
Marwan Qureshi
Beverly Romeo-Beehler
Jagannath Sharma
Shilpa Sharma
Roman Shcherbiuk

Ravjeet Singh
Colin Song
Enguerrand Sudrat
Wen Tao Suo
Claresta Apriria Sutanto
Maria Tayenjam
Kuan Thurow
Elise Kwok Ling To
Badri Vijayaraghavan
Sarah Wamil
David John Ward
Yan Wu
Luling Zeng
Jiadi Zhang
James Zhou

Canary Islands

Ben Irvine

Cayman Islands

Megan Renee Argenbright
Camila Rodrigues Costa
Candice De Coteau
Latoya Lovitta Francis
Sabina Caridad Hydes
Lilian Kanijo
Noela Lucian
Gwinyai Masiyiwa
David Raphael Milimo
Irene Mosonik
Racene Persad
Hayley Powell
Everton Paul Spence
Jade Wheeler

Chile

Xinlei Zhuang

China

Maofeng An
Wing Yan Au
Shijie Bai
Shilong Bai
Beilin Bao
Moyi Bao
Yucui Bao
Yuliang Bi
Yarui Bian
Jingqiong Cai
Zhuozhen Cai
Xinkai Cao
Hanhui Chen
Hao Chen
Huanwei Chen
Jian Chen
Jingjing Chen

Juan Chen
Junli Chen
Junyi Chen
Lei Chen
Lei Chen
Li Chen
Liru Chen
Maoyong Chen
Meiyong Chen
Meng Wen Chen
Na Chen
Peibin Chen
Shaomin Chen
Songxue Chen
Xi Chen
Xi Chen
Xiaoxia Chen
Xiu Chen
Xiuling Chen
Xueying Chen
Yue Chen
Ze Min Chen
Zhu Chen
Zimeng Chen
Chenzi Cheng
Meng Cui
Tong Cui
Hao Dai
Jieyu Dai
Qian Dai
Zhihua Dai
Dan Deng
Yue Deng
Wei Ding
Xuemei Ding
Yan Ding
Huaying Dong
Jingliang Dong
Ming Dong
Panpan Dong
Wenjia Dong
Shihua Dou
Zhengjian Dou
Caijin Du
Lirong Du
Shaojun Du
Sihan Du
Hanwen Fan
Sha Fan
Tingze Fan
Yuhong Fan
Zhihong Fan
Fei Fang
Hui Fang
Min Fang
Danting Feng
Jie Feng

Li Feng
Liwen Feng
Xiaoja Feng
Mi Fu
Rao Fu
Xiabin Fu
Xiaoqiang Fu
Xinlan Fu
Li Gao
Teng Gao
Xin Gao
Xin Gao
Yanfei Gao
Yiwen Ge
Yao Gong
Zhen Gong
Liyuan Gou
Boyi Gu
Chao Gu
Chengqi Gu
Fankai Gu
Shuai Gu
Yuan Yin Gu
Chunjing Guo
Feng Guo
Jian Guo
Lin Guo
Mengxiao Guo
Ting Guo
Weiping Guo
Wenxia Guo
Xin Guo
Yingying Guo
Jie Han
Pingsuo Han
Shihai Han
Kun He
Liu He
Qili He
Xinying He
Mei Hong
Mei Hong
Mengyuan Hong
Xishuo Hong
Fei Hou
Yangfan Hou
Yatong Hou
Zhangmeng Hou
Qianying Hu
Wenqian Hu
Xiaoming Hu
Xinhao Hu
Xiyu Hu
Zhenhua Hu
Jiaping Hu
Kenan Huang
Man Huang

Pujing Huang
Qiaoling Huang
Tingqing Huang
Wentan Huang
Wenzhu Huang
Yun Huang
Zixin Huang
Ying Huo
Meijun Ji
Qian Ji
Ruiru Ji
Tianyi Ji
Wenhan Ji
Xiaoting Ji
Zhi Ji
Lili Jia
Yufan Jia
Liangjiao Jiang
Mingyi Jiang
Nan Jiang
Qianqian Jiang
Shan Jiang
Minxi Jiao
Mengran Jie
Chaoqing Jin
Chengyu Jin
Wei Jin
Wenjuan Jin
Xuezhe Jin
Zefu Jin
Zonghan Jing
Zhu Junlin
Ziwei Lai
Xinxu Lan
Yong Lan
Lei Lei
Yawei Lei
Bo Li
Bo Li
Chenxin Li
Chenxu Li
Chuanmei Li
Chunlong Li
Fen Li
Frank Li
Hongbo Li
Jia Li
Jiangyue Li
Jiawen Li
Jingzhuo Li
Junlan Li
Li Li
Lu Li
Mansi Li
Meng Li
Mengyu Li
Min Li

Na Li
Panwen Li
Qi Li
Qian Li
Qiang Li
Qing Li
Ruiwen Li
Shuyi Li
Shuyu Li
Siqi Li
Siyong Li
Tianqi Li
Weitong Li
Wenrui Li
Xinyang Li
Xue Qin Li
Yali Li
Yanfei Li
Yatao Li
Yimeng Li
Yuanjie Li
Zhe Li
Bin Liang
Lihuan Liang
Qiaoying Liang
Ruichen Liang
Yanshan Liang
Yuan Liang
Chunhong Liao
Taitao Liao
Zhenzhen Liao
Haijiang Lin
Junwei Lin
Qiangdong Lin
Song Lin
Yueqi Ling
Chunbo Liu
Chunjie Liu
Chunming Liu
Dan Liu
Fangru Liu
Hao Liu
Jingfen Liu
Junjiang Liu
Li Liu
Ling Liu
Lu Liu
Mingjuan Liu
Naijia Liu
Qiancen Liu
Qirui Liu
Shuailing Liu
Shuyang Liu
Tianyu Liu
Ting Liu
Tingting Liu
Xiaoliang Liu

Xinyuan Liu	Juanjuan Qi	Fan Wang	Pei Wu
Xinyue Liu	Kai Qi	Fei Wang	Siqi Wu
Xiufan Liu	Yuran Qian	Hailei Wang	Xiaohua Wu
Yanbei Liu	Haiying Qin	Han Wang	Yan Wu
Yang Liu	Sijia Qin	Hanle Wang	Yang Wu
Yanqi Liu	Shi Rao	Hui Wang	Yao Wu
Yejun Liu	Kai Ren	Jiayi Wang	Yuanyuan Wu
Yichun Liu	Kexin Ren	Jingni Wang	Zhijun Wu
Yijin Liu	Yingchan Ren	Jue Wang	Ruoyun Xi
Yiran Liu	Kehang Shang	Junjie Wang	Shan Xi
Yiwei Liu	Liang Shang	Kaiqi Wang	Pingli Xia
Yufeng Liu	Qinghai Shao	Kechang Wang	Qiyue Xia
Yuhong Liu	Yanqun Shao	Kun Wang	Xiaoyan Xia
Yuying Liu	Zhan Shao	Lisheng Wang	Yuzhou Xia
Zhaoqiang Liu	Jing Shen	Lu Wang	Yu Xiao
Ziqian Liu	Ping Shen	Mingtao Wang	Baokun Xie
Xiao Yu Long	Shuangshuang Shen	Qiang Wang	Kang Xie
Xuejiao Lou	Linghong Shi	Qun Wang	Linna Xie
Yun Lou	Qianqian Shi	Rui Wang	Lujia Xie
Chengdi Lu	Shuwei Shi	Rui Wang	Weiwei Xie
Dengfei Lu	Xuhua Shi	Ruiqi Wang	Wenhua Xie
Guanhua Lu	Yuanyuan Shi	Run Wang	Ke Xing
Guiyi Lu	Shuang Shu	Shiyue Wang	Hao Xiong
Haiyan Lu	Jinling Song	Shu Wang	Qiangqiang Xiong
Yuanshan Lu	Yan Song	Shuyu Wang	Ao Xu
Yunqi Lu	Yilong Song	Ting Wang	Bingjie Xu
Zhangyu Lu	Zhaoyi Song	Wei Wang	Fangjing Xu
Dongchuang Luo	Zhiyi Song	Weixuan Wang	Haiying Xu
Jingting Luo	Bo Su	Wenjun Wang	Huan Xu
Xu Luo	Shuang Su	Xia Wang	Jieying Xu
Xueliang Luo	Tingting Su	Yan Wang	Jun Xu
Chen Lv	Wenjin Su	Ye Wang	Se Xu
Guobao Lv	Yang Su	Yi Wang	Shanshan Xu
Xinxin Lv	Huihui Sun	Ying Wang	Sishi Xu
Yang Lv	Jiuyan Sun	Ying Wang	Wangyan Xu
Yuhong Lv	Linlin Sun	Yingeng Wang	Xiaojie Xu
Zhuqi Lyu	Mingyang Sun	Yuanyuan Wang	Xiaomei Xu
Chaoning Ma	Nan Sun	Yujue Wang	Xiaomeng Xu
Ji Ma	Rongfei Sun	Yunqiao Wang	Xiaoyu Xu
Jiangni Ma	Xiubing Sun	Zehang Wang	Yihang Xu
Na Ma	Yao Sun	Zheng Wang	Yun Xu
Shanxiang Ma	Ying Sun	Zhexin Wang	Yuwen Xu
Min Mao	Shiyin Tan	Zhiyu Wang	Yuzhu Xu
Haodong Meng	Sijing Tan	Zhongkui Wang	Zinan Xu
Wei Ni	Kaijie Tang	Mengyi Wei	Ying Xue
Phoebe Nie	Li Tang	Peilan Wei	Bing Yang
Xiaoming Nie	Shi Tang	Shaoheng Wei	Haodi Yang
Fengzhen Ou	Xiaoping Tang	Cheng Wen	Hongyan Yang
Jiali Pan	Yunli Tang	Yang Wen	Jin Yang
Jingyi Pan	Zhihao Tang	Fang Fang Wu	Jun Yang
Jinxin Pan	Wanming Tao	Haobo Wu	Kaixuan Yang
Sicheng Pan	Ye Tao	Hongjie Wu	Ling Yang
Wen Pan	Ye Tian	Jianzhou Wu	Qiuyang Yang
Yongjie Pan	Chen Wang	Jiayi Wu	Shiyu Yang
Zhengjun Pei	Dan Wang	Kefei Wu	Xi Yang
Si Peng	Dantong Wang	Kerui Wu	Xiaofang Yang
Xiaotian Pu	Dongzhi Wang	Nan Wu	Xuefei Yang

Yi Yang
Yuhan Yang
Yunting Yang
Yuting Yang
Yuxi Yang
Dingding Ye
Jing Ye
Xia Ye
Yu Ye
Chao Yin
Fangwei Yin
Yi Yin
Yixuan Yin
Huishi Yu
Jintao Yu
Lan Yu
Wen Yu
Xiaochen Yu
Yu Yu
Zhuxin Yu
Na Yuan
Shuhan Yuan
Tingyao Yuan
Wenhui Yuan
Ye Yuan
Tingyan Yue
Shichao Zhang
Yalei Zang
Wanni Zeng
Li Zha
Xi Zha
Dongying Zhan
Kai Zhan
Liang Zhan
Bo Zhang
Cailing Zhang
Chenrui Zhang
Haigang Zhang
Hailong Zhang
Hongyan Zhang
Jing Zhang
Jingqiu Zhang
Li Zhang
Liangxue Zhang
Lin Zhang
Ling Zhang
Liu Zhang
Mingming Zhang
Mingsheng Zhang
Nianwei Zhang
Pengjiao Zhang
Qingyuan Zhang
Qiyue Zhang
Ran Zhang
Rui Zhang
Shenjun Zhang
Shuang Zhang

Shuoxuan Zhang
Xia Zhang
Xiaolei Zhang
Xiaoru Zhang
Xinqi Zhang
Xinyu Zhang
Xurong Zhang
Yan Zhang
Yanjuan Zhang
Yaoshong Zhang
Ying Zhang
Yinlong Zhang
Yongheng Zhang
Yuan Zhang
Yue Zhang
Yue Zhang
Zhicheng Zhang
Bingqing Zhao
Changlin Zhao
Fangchao Zhao
Jigang Zhao
Kai Zhao
Lijuan Zhao
Qing Zhao
Sha Zhao
Shuhui Zhao
Xianli Zhao
Xin Zhao
Xuezheng Zhao
Ying Zhao
Yingying Zhao
Yun Zhao
Zhen Zhen
Guanghua Zheng
Jingjing Zheng
Lei Zheng
Mengjie Zheng
Tong Zheng
Xinhui Zheng
Xinruo Zheng
Zibo Zheng
Chenyi Zhong
Huizhi Zhong
Baixuan Zhou
Caihong Zhou
Chen Zhou
Chen Zhou
Fan Zhou
Honghong Zhou
Huocheng Zhou
Jiachen Zhou
Jianmei Zhou
Jingwei Zhou
Ya Zhou
Yiyuan Zhou
Yuancheng Zhou
Yucai Zhou

Ziqing Zhou
Ziyuan Zhou
Chang Zhu
Huajun Zhu
Hui Zhu
Jigao Zhu
Li Zhu
Lin Zhu
Shengnan Zhu
Xingyu Zhu
Yi Zhu
Yong Zhu

Colombia

Liebermann Lozano

Costa Rica

Erick Alpizar
Eddy Chavarría Ruiz
Gerardo Chavarria Salas

Curaçao

Mitchel Brunings
Dennis Engelhardt
Sharmine Major
Zulay Martina
Elisabeth Romer
Frandyeska Wall

Cyprus

Despo Pampaka

Czech Republic

Giulia Castoldi

Dominica

Julie-Ann Charles

Egypt

Ahmed Abdelaal
Eshraq Abou El Enein
Mohamed El Ghorraieby
Shady El Said
Dalia Elkady
Wafaa Kandil
Mohamed Magdy Elkholy
Atef Osman

Estonia

Hanno Parksepp

Finland

Stuart Mooney

France

Imane Badi
Fatima Belmir Billard

Carole Diane
Viktor Djongov
Marine Schneider

Germany

Alexander Bergmann
Fabian Best
Hergen Frerichs
Youxuan Gao
Yannick Gobelbecker
Shu Han
Andreas Pilger
Theresa Riehm
Janusz Ryzner
Natalie Salamova
Romina Stuhmann

Ghana

Norberta Bavor
Ivy Kpodo
Gideon Kyei
James Kingsley Owusu
Amos Sackey

Greece

Christiana Giannakoura

Guyana

Colette Adams

Hong Kong

Aimee Chan
Cheuk Ling Chan
Hong Yiu Chan
Io Kit Chan
King Kok Chan
Ping Ying Chan
Puilam Chan
So Shan Chan
Tsz Wai Chan
Jingyi Chen
Chi Cheng
Ka Chun Cheng
Ka Ngai Cheng
Pang Ming Cheng
Chin Pong Cheung
Rachel Chi Lam Choi
Yau Ming Choi
Hiu Yu Chong
Ka Man Chow
Ka Yi Chow
On Ki Chow
Cheuk Yin Chui
Wing Mei Chung
Ellie Hei Wai Fok
Ilario Francescutti

Siu Chung Ho
Wing Kwan Ho
Li-Nien Hou
Chi Yuen Ko
Shum Yee Jessie Kwai
Joanna Kwan
Tsz Hin Kwok
Wing Yu Kwok
Hau Ching Cheryl Lam
Ho Lim Lam
Kai Wing Lam
Lai Kwan Lam
Oi Kiu Ankie Lam
Tat San Lam
Wing Tung Raymond Lam
Yin Fai Lam
Chi Hang Lau
Sze Man Lau
Ka Chun Law
Marco Law
Wing Sze Law
Heung Wing Lee
Hyunjae Lee
Kelvin Lee
Kwan Wing Lee
Kwun In Jessica Lee
Wing Man Lee
Chi San Leung
Chin Kan Leung
Sin Yan Leung
Kin Sum Li
Haifeng Liu
Siu Hei Lo
Yuk Lin Lo
Liyin Lu
Di Ma
Tsz Hin Man
Jason Mok
Hoi Yee Agnes Ng
Ka Wing Karen Ng
Sze Kei Ng
Ka Ming Ngan
Wing-Shun Hester So
Kwok Yiu Raymond Suen
Chi Yan Sara Tong
Hei Wun Tong
Wai Naai Tong
Yat Fung Tsang
Wing Yin Tse
Suet Him Carly Tsui
Lawrence Sin-cheung Wai
Xuhui Wang
Hiu Tung Wong
Tsz Toa Wong
Vivian Wong
Zhong Yuan Wu
Sik Sik Yeung

Wai Leung Yeung
 Nga Ying Yeung
 Yuen Yiu Yeung
 Kai Hong Yip
 Chui Kwan Yu
 Pui Sung Erika Yuen
 Ka Ming Yuen
 Tsz Kwan Yuen

India

Nisha Agarwal
 Arvind Anand
 Geeta Bhandari
 Nipun Indravadan Bhatiya
 Kanishka Bhatnagar
 Prashant Anna Bidkar
 Akhil Chaturvedi
 Harpreet Singh Chhabra
 Naveen Kumar Chinthakindi
 Sandeep Choudhary
 Amar Das
 Kranti Kanyaka Das
 Geetanjali Dofara
 Vijay Ganesan
 Amar Nath Gupta
 Madivalayya Hiremath
 Anil Kumar Jain
 Aarti Jha
 Akshay Joshi
 Shaffy Kalra
 Ravi Kanchi
 Abhishek Kapoor
 Anu Kaushal
 Assifulla Khan
 Rajasekhar Kolli
 Nirmal Kumar
 Rajiv Kumar
 Sandeep Kumar
 Sawan Kumar
 Jyoti Aaditya Maheshwari
 Alkaf Memon
 Javeed Mohammad
 Mohammed Zakir Mohideen
 Kurumuju Nagarjuna
 Balantrapu V. Naga Raja Nandini
 Sachin Nema
 Sreedhar Nethula
 Tushar Suresh Pande
 Ganesh Prabhu
 Aparna R.
 Karthik R. N.
 Abhinandan Rai
 Jyotsna Rajpal
 Govind Ramakrishnan
 Eedulakanti Ranadeep
 Amal Reji
 Sayyad Rijwana Begum

Habeeb S.
 Vishnukanth S.
 Srikanth Sridharanambi
 Avae Mariya Stalin Santhiyagu
 Manali Santra
 Charishma Sathyaprabhu
 Amrendra Kumar Singh
 Jishnu Menakath Sivasankaran
 Prabhu Sreenivas
 Rajol Tavade
 Sharad Vyas

Indonesia

Deni Bayu Ardi
 Wikan Karis Basutama
 Kiki Fauzia Bidari
 Riko Putra
 Vikram Singh Rathore

Ireland

Natalia Gburzynska
 Daire Seosamh Lee
 Alan Mangan
 Adeoye Onikan
 Ruth O'Regan
 Eoghan Quinn
 Jesus Aaron Ruiz Zapata
 Danielle Sherry
 Alexandros Tsilipanos
 Xin Wang

Italy

Enrico Bleve
 Omar Tavana

Jamaica

Mark Anthony Lyons
 Cordella Medley Gayle
 Sanetta Swaby
 David Ralston Swaby

Japan

Mizuki Ayabe
 Saki Fujioka
 Masayo Fukuchi
 Yukihiro Hagiwara
 Hiroaki Hashiguchi
 Daiki Kawamata
 Mikiko Kobayashi
 Takahiro Komoto
 Sohei Kuramoto
 Hiroshi Maekawa
 Kenta Masuno
 Bishnu Prasad Neupane
 Masatoshi Norimoto
 Emi Ozaki

Takaaki Saito
 Yuko Saito
 Yuta Sato
 Takehiko Senju
 Yukiji Shindo
 Yoshihiro Shinomiya
 Mi Young Song
 Takahiro Sugita
 Hirofumi Suzuki
 Denis George Sweeney
 Soji Takano
 Seiji Tamai
 Eiji Umemura
 Mami Yamamoto
 Tomomi Yamashita
 Akihiko Yokota
 Atsushi Yoshida
 Yuji Yoshida
 Kwun Lok Kingson Yuen

Jordan

Tagwa Ahmed
 Tareq Ahmad Al Damisi
 Eman Mohammad Al Fawair
 Mohammad Musleh Al-Disi
 Rania Salah Eldin Elkhalifa
 Romaisa Haj Eldaw Hamid
 Abdalaziz Mohamed Omer

Kazakhstan

Zhaniya Turlobekova

Kenya

Noel Lukela Benerdict
 Chemutai Jackline
 Kizito Kariuki
 Soi Kiprotich
 Jeniffer Mutinda John
 Maxwell Kibaso Machira
 Nicholas Maina
 Gloria Nabwire Mumoki

Kuwait

Noor Alfares
 Saad Almenifi

Laos

Chatouphone Chanthasaly

Latvia

Ilja Brehovs
 Jekaterīna Ptičkina

Lithuania

Darius Rindinas
 Tomas Zubernis

Luxembourg

Alexis Godefroy
 Mihaela Popova
 Yurika Sato
 Amedeo Trovarelli
 Yingcen Yang
 Lian Zuo

Macau

Hoi Neng Au Yeung
 Ka Man Chao
 Jing Chen
 Hoi Tek Cheong
 Weng Sai Leong
 Jie Lin
 Sio Wai Lio
 Biao Wen Mai
 Wu Man Chon
 Sin Mei Ng
 Shuyan Tan
 Im Heng Wong
 Iwai Wong
 Yunfu Xie

Malawi

Lancy Asedi

Malaysia

Hana Atikah Binti Hamzah
 Chun Hou Koh
 Chui Yin Low
 Boon Kia Seow
 Shuhaira Shaidan
 Andrew Shean Liang T'ng

Malta

Spyridon Chrysochoidis
 Glenn Gauci
 Chiajen Lin
 Mauritius
 Sanjun Guo
 Lei Yang
 Jianping Zhang

Mexico

Jose Luis Lopez Ruiz
 Agmet Miguel

Nepal

Suyash Arjyal
 Amit Man Shrestha

Netherlands

Berenice Acosta Hernandez
 Üsame Ceylan

Leandro Fernandez Gonzalez
Wei Shan Hii
Juliette Hipp
Aleksandra Kaminska
Oleksandra Levchenko
Roushnie Shahatoe
Tim van de Watering
Nikita Vlasman
Casper Weijs
Tara Yaco Chamoon
Yibo Yang

New Zealand

Rupali Barboza
Hon Chun Chan
Giulia Dondoli
Tina Fu
Jorgia Gallagher
Katie Gartside
Rebecca Ma
Ben McAlpine
Kelly Quach
Natalie Stagg
Emily van Arendonk

Nigeria

Victoria Adelugba
Solomon Akhimien
Chukwuma E. Nweke
Ismail Ajegbenga Olaleye
Ayodeji David Olulode
Uchenna E. Onyenakasa
Ganiyat Mopelola Seriki
Jimada Muhammad Yusuf

Oman

Omar Al Raisi

Pakistan

Sameer Lalwani
Sidra Latif
Amer Nawaz
Muhammad Aman Yaqoob

Palestinian Territories

Maen Hajir

Paraguay

Javier M. Ferreira Speratti
Luciana Rierra Encina

Philippines

Stephen Baysac Colobong
Ma. Lourdes O. Dino
Michael Habacon Lindayag

Gina Rose Ycasiano

Poland

Rafal Cybulko
Adam Kaczor
Bartosz Ostrowski

Puerto Rico

Mahisy Perez Albino
Mark Paul Weisenborn

Qatar

Maisam Abdelaziz
Syed Noman Ahmed
Treysi Alkac
Issa Daas
Vikram Liya
Akhter Lone
Mohamed Mahmoud
Haris Manzoor
Khurram Shah Mohammed
Tugce Ozbey Gurkan
Sharifa Ticklye

Saint Lucia

Tamara Maynard-Henry

Saudi Arabia

Sada Bint Khaled Al Saud
Anhar Abdullah Alwusaydi

Serbia

Sandra Giba

Sierra Leone

Ozobia Samuel Davies

Singapore

Jermayne Ang
Marcus Wei Jie Ang
Yik Han Ang
Chrysan Chan
Chiat Yee Chia
Lee Moy Chong
Chua Chua
Keith Chua
Divya Das
Ozobia Samuel Davies
Bing Xuan Bryan Goh
Eng Puay Michelle Goh
Kaanchi Gosalia
Chien Ming Kelvin Ho
Sheue Lee Hoh
Jong Hwee Jonathan Kho
Mun Keong Koh
Yeow Sin Koh

Priyanka Kumari
Shu Hui Lim
Jiayao Desmond Lin
Juehai Lin
Forgel Looi
Eileen Lum
Li Fang Rozanna Lum
Ka Yu Victoria Ng
Min Min Ng
Rita Niranjani
Shermon William Ong
Ruben Bennett Potter
Gary Lim Quan
Zhengcai Jason Quek
Ilham Rasman
Chiau Hwa See
Lip Leng Calvin Seow
M. Subrahmanyam
Kiju Sung
Waseem Syed
Leung Tak Poon
Peng Wei Tan
Tina Qi Jin Tan
Jia Le Teng
Wan Yi Teo
Yuan Chyi Teo
Jessica Toh
Toh Hong Tu
Jiamei Wu
Kin Man Yan
Song Qi Joel Yeo
Tat Zhun Yip
Cheng Liang Yong
Jinshu Zhang

South Africa

Tarryn Ford
Liang Jiao
Cassim Joona
Lesedi Kgopong
Patricia Malongo Mbelu
Lerato Cynthia Mongane
Abdullah Moses
Lesego Seeletso Tamenti
Kashnie Naidoo
Firdaus Noorshib
Sibongile N. Sambo
Marcus Swanepoel
Dumiso Vilakazi

South Korea

Maromi Ahn
Hajin Bae
Junhwa Cha
Seung Hyeon Cho
Yunsoo Cho
Yunji Choi

Jingwan Ha
JungEun Han
Soo Yeon Han
Seongwook Hong
Kye Yean Hwang
Jeong Won Jang
Hyojoon Jeong
Jaehee Jeong
Jihye Jeong
Juhyun Jeong
Soyeon Jeong
So Jiyoan
Hee Jeong Kang
Hee Soog Kang
Tae Hun Kang
Yunsung Kang
Ae Jung Kim
Chae Yeong Kim
Dahye Kim
Dajeong Kim
David Hyunwoo Kim
Eunkyung Kim
Hong Kyu Kim
Hongseong Kim
Jan Di Kim
Jeongnim Kim
Ji Hyun Kim
Jihye Kim
Joungsuk Kim
Minjeong Kim
Soran Kim
Yoo Kyoung Kim
Yuseon Kim
Hyerin Ko
Kwangrim Ko
Guma Kwon
Jieun Kwon
Cheongyeon Lee
Seung Meong Lee
Bumju Lee
Jinha Lee
Jinwoo Lee
Kyu Hyun Lee
Sumin Lee
Young Ri Lee
Jinhee Moon
Song Myounghee
Muntae Oh
Myeong Hun Park
Sujeong Park
Sunhee Park
Hyeong Jun Seo
Mijeong Seo
Eunho Seong
Yuri Shim
Jiwoo Shin
Soo Jung Sim

Joonhyeok Son
Eun Im Song
Myounghee Song
Aekyoung Yeom
Jaemin Yi
Ye Rin Yoon

Spain

Aymeric Lemesle

Sri Lanka

W. Krishan W. Gunathilake

St. Kitts and Nevis

Terence Raymond Craig
Shawn K. Richards
St. Vincent and Grenadines
Enika Jillian Peters

Sudan

Thoria Gismallah

Switzerland

Vairea Baur-Roby
Emilie Bitoun-Elkaim
Jacqueline Eggenschwiler
Sandy Lavorel
Md. Zahed Uddin

Taiwan

Chung Kai Chang
Hui Wen Chang
Hui Wen Chang
Pang-Yu Nathan Chen
Ya-Li Chen
Tzu Po Venson Chien
Mei-Chun Maggie Cho
Shan-Chin Chu
Chun Ling Chueh
Ya-Hsin Hsiao
Bo Kai Huang
Sheng-Ming Huang
Yen Ting Lee
Ya-Jhen Li
Shih Hung Lo
Clair Pan
Pin-Hui Su
Hsin I. Tsai
Pei-Chun Tsao
Hsin Yi Tseng
Yu-Chen Wang
Yu-Chiung Wang
Jia-Syun Wu
Chen Yu Wu
Yen-Ju Yang

Thailand

Thanachot Leelasuwongvong

Trinidad and Tobago

Capil Davin Boodram
Pradesh Jaimungalsingh

Turkey

Yunus Emre Özgül
Elvan Öztabak

Uganda

Nisa Allena Ankunda
Evelyn Fiona Namulondo
Pauline Nyapendi
Patrick Okettayot

Ukraine

Vadym Romaniuk

United Arab Emirates

Yasmine Abdelhamid
Ilyas Karuppamveettill Abdu
Ahmed Mohamed Abuelmaaty
Manjusri Achuthan
Dildar Ahmad
Syed Jamil Ahmed
Linda Amoit Amuke
Sangeetha Arun
George Alexan Fahmy Ayad
Sreekumar Bhaskaran Nair
Ankitha Byndoor Vasudeva Navda
Blessy Chacko Ancy
Manu Cleetus
Charmaine Colaco
Parbati Dhakal
Muhammad Ali Khan Durrani
Ahmed Elisawi
Mahmoud Elmaghrabi
Nidhin Gangadharan
Varughese George
Jaypee S. Hamili
Abdalla Haroun Elayouty
Mustafa M. Mustafa Hassis
Shahin Iqbal Ibrahim
Awatef Ismail
Mohamed Shebil Ismail
Nija Jacob
Aqeel Jaffery
Raavi Jain
Remya Jose
Dinesh R. K. Kalinga
Anubhav Kapoor
Varinder Khanna
Ram Kumar

Shibin Kuttassery Sivadasan
Judith Mae Lorena
Ali Raza Mehdi Khan
Taizoon M. Merchant
Mahammad Nadeem
Girish Gopalakrishnan Nair
Jean Baptiste Neel
Kennedy Omondi
Anees Rahman Palliyali
Samuel Pitchai Peter
Michelle Andador Rafeiro
Nidhin Ramesh
Shamili Jeniffer Ravindra Singh
Eva Malisha Rodrigues
Pradeep Roshan
Vinay Sandhu
Shubham Sharan
Soumya Shukla
Nilay Ranjan Singh
Yifan Song
Mohamed Sheik A. Syed Ibrahim
Dawn Thomas
Mahesh Uragala
Ritika Vaid
Ajitha Ana Varughese

United Kingdom

Ngozi Akalawu
Edward Anku
John Philip Barbarich
Santa Busujeva
Gavin Caldwell
Sergio Cavallo Vayda
Hsi-Yu Chen
Harriet Christodoulou
Seyra Kodjo Tsatsu Dagadu
Fanjin Feng
Murad Hasan Hamzo
Nick Henderson
Hanui Hong
Phil Larratt
Wing Sum Vincy Leung
Wenbei Liu
Surbhi Mahajan
Neethu Manish
Martin McConville
Chijioke Oforji
Annuncieta Onyinye Okolo
Wahidollah Saft
Feyisayo Yewande Savage
Nicholas Smith
Katherine Ward
Abdullah Warsame
James David Whisker
Jin Zhao

United States

Mahnoor Abbasi
Pamela Abernethy
Shadiat Morenike Adebisi
Adeyinka Abeeb Adelekan
Niyi Adereti
Tolulope Akinola Agboola
Aramjeet Agnihotri
Sindy Aguirre
Fatimo Mary Ajiboye
Joseph Oyewole Ajiboye
Mikaela Alcalá
Aria Alexander-Manifold
Olanrewaju Mark Aluko
Karen Alvarado Lopez
Kimani S. Anderson
Wendy Anderson
Michael R. Arison
Andrew Nicholas Armstrong
Sharreye Askins
Mitchell Atilés
Akeel A. Babar
Zahratu Bah
Jessica Bailey
Bryce Becker
Daniel L. Bell
Stephen Bethoney
Nick Betsinger
David Binkley
Erin Blakemore
Marshall Boden
Deborah Bolarinwa
Judy Bornebusch
Stephanie R. Bowers-Legg
Samuel H. Boykin
Ryan Peter Brennan
Hunter Brown
Hazel Geneva Brown
Jamie Buchinski
Christopher Burns
Evan Burt
Katy C. Cabrera
Johanna Caceres-Mendez
Nancy Cadwallader
Daniel Camaj
Michael David Camilleri
Matthew Campioni
Kimberly Canales
Andrew Canavero
Brian W. Cauty
Connie Cashion
James Castano
Connie Nichole Castillo
Eleanor Castoro
Andrew W. Cave
Manhong Chan

Yen Chen Chiu
Gini Chukura
Danyl Chung
Carla Clary
Eric Cohen
Hilary Cole
Miriam A. Cole
Robert Jason Cole
Eric Collazo
James Collings
Hector X. Colon
Andrew Charles Colston
Alison J. Conklin-DeVita
Kelsey L. Conn
Kristie Cook
Laura Michele Cooley
Victoria Cooper
Matthew Coughlin
Remington V. Creamer
Kristopher Criado
Patrick Cunningham
Harish Dakshinamoorthy
James Maxwell Daniels
William Davidson
Jackilyn Anne Felipe Davis
Lyubov Davis
Andrew S. Davis
Henderson Eddie Days
Sierra Dehmer
Danielle DeLeon
Robert Delia
Heather L. DeMinck
Ashley P. Demorest
Joseph D. Deo
James Devoe
Nirmit Dhalgara
Ruby Diaz
Tina Dinelli
Troy Divine
Ivan Dolgonos
Aaron Dorfman
Tasha Nicole Drake
Julie Earls
Oluyemi Kunle Elegbede
David T. Ellingson
H'Driet Enuol
Eda Erol
Cole Evans
Lesley Anne Evans
Enumah E. Eze
Brandi Farrer
Luke Q. Fearey
Alissa Fernandez
Marion Foucher
Ashley Fry
Televi Fumey

William Andrew Furay	Andi Ibro	Prakash Reddy Mannuru	Neha Pandhre	Maya Kennebrew Small
Rebecca Elizabeth Fuson	Uboho Emmanuel Inyang	Nicole Marie Marcischak	Prajakta Paradkar	Ida Maria Smith
Federico Garcia	Eric Jacobs	Jonathan M Martinez	Disha Parikh	Robert L. Soria
Jean Pier E. Garcia Dorta	Thomas James	Julia Lauren Martinez	Cesar Perez	Olivia Spencer
Karla Gava	Melanie Jean	Melissa Maynard	Priscila Pesek	Nathan Richard Spinder
Tyler Gelfand	Colina S. Jehdian	William E. McCausland	Tanya F. Walwyn Peterson	Zvezdana Stamenkovic
Nicholas Daniel Gennarino	Robert Hiatt Jessup III	Alexis McClure	Adam Petralli	Bethany Ann Stanger
David Christian George	Jason Patrick Johnson	Melissa McCormick	Timothy J. Pfund	Gary Stevens
Leea Gibson	Mariah Johnson	Frederica McGinnis	Kim-Yen Phan	Lucas Stokes
Jean-Marie Gillette	Alexis Jones	Sara McKie	Robert Phillips	Michael John Suspenzi
Mariam Gillis	Andrew Ned Jorgensen	Barry D. McKinley	April D. Phillips	Jonathan Szeliga
Dylan Giordanengo	Quinn Julian	Demetrius McKinney	Brett Pinnix	Teniola Taiwo
Jamie Glatthorn	Byeongil Jung	Erik McLaughlin	Kristen Anne Poitevin	Karl Stephen Tarrant
Rebecca Ann Glenn	Sarah Karagias	Thomas McLoughlin	Tyler Polley	Jenny Tasavanh
Melanie R. Goldberg	Sebnem Karakurt	Derrick Michael McPherson	Cinnamon A Pool	Dillon Taton
Wendy Paola Gomez-Castillo	Steven Katsev	Gregory A. McWard	Fernando Powell	Bryant Taylor
Rebecca Gonez	Alina Kazakovtceva	Natalie McWilliams	Margaret Powers	Aryand Thuelen
Erick Gonzalez	Kenneth Robert Key	Larry Mercado	Emily Purnell	Ericia Joy Thomas
Aaron E. Gonzalez Garcia	Amy Kieper	Alexander Wayne Meyers	Melanie Pyanowski-Skeels	Floyd Thompson
Emarilis González González	Shion Kim	Nicole Michaels	Cesar Quintero	Deryk L. Tran
Daniel Gonzalez Wibling	Minji Kim	Brittany Miller	Khizar Qureshi	Shelby Tudor
Monica C. Gonzalez-Curci	Quintin Kime	Charles Louis Miller	Courtney Ragan	Joshua Uyanga
Shannon Latrice Graham	Mark Kleynerman	James Miller	Ananda Ram	Eduardo H. Veiga Jr.
Andrea R. Grant	Jeffrey Knight	Phillip L. Mimnaugh Jr.	Elizabeth Ranft	Donna Vereen
Karlie Griffin	Carol C. Knowles	Viswanathan Mohan Iyer	Anjali Raturi	Justin Paul Volk
Kevin Grimes	Yulia Korin	Michael Anthony Molnar	Seth J. Reister	Harry Wagner
Grant Gulickson	David J. Kroot	Elizabeth Jordan Moore	Elizabeth S Rice	Justin Walder
Kendra Lauren Haar	Thomas Kurtz	Pedro Maria Morales Aizpun	Amanda Rivas	Chelsea E. Mary Waterson
Matthew Hagen	Sheri Laboe	Lynette Real Moroney	Joseph Roberts	Keldon Watts
Kehinde Hamed	Ellen Wingyan Siu Lau	Edward M. Moseley	Kristy Rodriguez	Steph Weaver
Hunter Xavier Hamon	Abhishek Cornelius Laxman	Adriano U. Mucelli	Sally Rork	Scott Weiser
Michael Joseph Hanhauser	Lauren Pikman Lee	Juan Munoz	Jordan Rose	Nathan Werre
Erica Hanichak	Kyungmi Lee	Lawrence James Murphy	Pamela C. Samsey	John Wesley
Drew Harless	Julie E. Lee	Jeminat Emoshoke Musa	Scott Andrew Samuels	Aaron Wickersham
Jessica M. Harris	Jane M. Lee	Muhammad Bilal Mustafa	Mackenzie Sanchez	Michael C. Wieczorek
Tessa Hart-Bonville	Heidi Lewis	Jorge Najera Flores	Taylor Sanders	Marissa Williams
Kevin Hartman	Brittany Lewis-Valverde	Sydney Nemecc	Alejandro L. S. Santana	Valerie Wilson
Timothy Patrick Hatfield	Chou Ngan Li	Anna Nesterowicz	Charlie Sashington	Courtney Michelle Windhorst
Trista Hayward	Seul Gee Lim	Christopher O'Bar	Gary R. Satterwhite Jr.	Sockeia Wise
Dustin Hellrung	Steven Alden Littleton	Ufuoma Ogunjumo	Jamie A. Schafer	Leonard Wiza
Julie A. Henthorne	Kristy Liu	Oluwabusola Uzo Ogunyode	Emily Scheff	Chennuo Wu
Jennifer Herbert	Inna Livshits	Elizabeth O'Halloran	Austin Schlechter	Jackie Yip
Ellen Herlicka	Pamela Logan	Adebisi Muiyiwa Olukoga	Susan Louise Schlosser	Adam L. Zamora
Zachary Herman	Margaret Lombardo	Bryan O'Neill	Jeffrey Carlson Schmid	Jared Dean Zarbinski
Janice M. Hernandez	Angelina Lopez	Franklin Onyenemerem	Nathan Schofield	Khaled S. Zhort
Kevin Hernandez	Sisley Lopez	Olanrewaju Oropo	Raymond Serion	Marion Zinowski
Juan Fernando Hernandez	Hang Lu	Katiana Ortiz	Yanina Sgroppo Emerick	
Amber Melissa Hill	Elizabeth Lucero	Cristina Ortiz	Ami Shah	Vietnam
Meredith Hinz	Sonya Luhm	Dennis Alexander Ott	Sonia Shankar	Khue Truc Lam
Samira J. Hitti	Beatriz Machado	Ayoade Victor Oyeleke	Orabia Shelby	Zimbabwe
Sara Hlebain	Tromila Lanise Maile	Joseph Ozag	Rebecca Sherman	Lovemore Kamuzangaza
Jillian Holmer	Kimberly Maines	Angel Ozerkov	Erica G. Savannah Shirey	
Micaela Hopkins	Arijit Asiskumar Majumdar	Jhagan Palanisamy	Chase Shurts	
Victoria Hulsey	Justin Male	Suresh Pallakonda	Daniel Silverman	
Krystal Hundt	Nitin Malhotra	Nateasha Palmateer	Arun Singh	
Daniel Curtis Hunt	Nathanael Mannone	Skyler Palmer	Shrddha Singhi	



CCAS GRADUATES: DECEMBER–FEBRUARY

Graduates' countries/regions are sorted alphabetically

Argentina

Gabriel Alejandro Chirinos

Bahamas

Rickel A. Trotman

Canada

Pierre-Etienne Balthazar-Lacasse
Colin Paul

Cayman Islands

Joel Alex Burke

Germany

Nico Di Gabriele

Hong Kong

Chan Pang Chung Daniel
Burnston Ping-Hang Fan
Ilario Francescutti
Wai Ming Yuen

Iceland

Thurstan S. Felstead

Ireland

Rodrigo Ignacio Montes
Sean Sheil

Japan

Makoto Tagaya

Jordan

Sameh Kamal AlQadi

Lithuania

Mantvydas Levickis

Malta

Chiara Cammelli

Nigeria

Mubarak Mohammed Abdullahi

Singapore

Ramesh Krishnamoorthy
Ignatius Tay Wei Chen
Zhao Qing

Switzerland

Matthias Greiller

Taiwan

Shu Yung Chien

United Kingdom

Stylianios Tachtatzis

United States

Chad Altieri
Joyce K. Batterson
Timothy Michael Cradle
Robert J. Grassau
Andy Guzman
Cory Houston Howard
Bryant Moravek
Raj Paul
Nissan Pow



SANCTIONS SPACE

A holistic solution for organizations to empower their workforce to remain compliant with complex sanctions laws.



The CGSS
Certification



Online
Training



Masterclass
Series



Monthly
Sanctions
Updates



Thought
Leadership



Networking

Explore these options at
acams.org/sanctions



CGSS GRADUATES: DECEMBER–FEBRUARY

Graduates' countries/regions are sorted alphabetically

Armenia

Ani Goyunyan

Australia

Nicole Biskop
Amanda Lui
Ben Moroney
Siqi Wu

Bahamas

Ashley T. Bethel

Bahrain

Abhilash Keloth

Bangladesh

Sagar Hossain

Canada

Aanchal Gulia
Jordan Hearsey
Xiaoxia Li
Camaro Mero
Wanqing Serena Shen

Cayman Islands

Wayne Alexander
Eoin Kennedy
Jessica Turnbull

China

Lingchun Cai
Jia Chen
Lin Chen
Xin Chen

Wei Dai
Lin Feng
Jintao Guo
Xiaowei Han
Yipeng Hong
Hongxing Jiang
Wanying Jiang
Xueying Jiang
Sha Li
Xiangxia Li
Ying Li
You Li
Yiwei Li
Yiwen Li
Wenjuan Liao
Baoquan Lin
Jing Liu
Liu Liu
Qi Liu
Simeng Liu
Xiao Liu
Yuwei Liu
Xiaomin Lu
Guizhi Ma
Jun Ma
Junfa Ma
Meimei Ma
Yun Ma
Liming Peng
Yu Shan
Xiaoyun Song
Rufei Su
Bincheng Sun
Dan Wang
Xiaoting Wang
Xinyang Wang
Yachao Wang

Yanmin Wang
Yongli Wang
Zhiyu Wang
Tingting Wei
Xiaojing Xian
Hao Xu
Yue Xu
Kun Yang
Lin Yang
Qier Yang
Yaohao Yang
Xinbi Zeng
Xu Zhai
Keshi Zhang
Sheyu Zhang
Wei Zhang
Wenjing Zhang
Wuyang Zhang
Yi Zhang
Yifang Zhang
Zhifang Zhao
Chen Zhong
Haiyun Zhong
Heng Zhou
Xiaochun Zhou
Hongye Zhu
Jiangning Zhu

Czech Republic

Jordi Rey Martínez

France

Xiaoshu Condonhe
Laura Marty
Lucile Pellissier

Germany

Michael Jarosch

Hong Kong

Ka Man Grace Chan
Chi Shing Hui
Nora Hui
Chun Pui John Kam
Gladys Ko
Ngat Chi Lau
Chung Hei Li
Hon San Lo
Balachandra Mysore
Judy Yuk Yee Poon
Sin Man Yam

India

Brahadheesh Deivanayagam
Swati Khandelwal
Praveen Kumar Nirmalraj

Ireland

Maria Azahara Cots Marfil

Israel

Anna Shrage

Japan

Tomoya Fujita
Naotoshi Okumura

Jordan

Omar Khier Al Jamal

Luxembourg

Timothee Didier

Macau

Junwei Ge
Shiu Man Simon Lee
Wai Long Wong

Netherlands

Leon Blonk
Ahmet Ferda Karadeniz

Norway

Heidi Hustvedt
Kristine Frivold Rorholt
Palestinian Territories
Anan Marwan Altif
Aseel Bader Qadi

Peru

Rodrigo Ruiz

Philippines

Edzen Jogie B. Garcia

Qatar

Ines Mohamed Sandli

Singapore

Vyara Chinnadurai
Tze Jian Joseph Kwek
Jasmeet Singh

South Korea

Giheon Ahn
Yeonju Choi
Saetbyeol Kee
Hyungsub Kim
Geunbo Ko
Hyerhin Lee
Hyoju Lee
Sanghee Lee
Hyecheon Na
Mihye Park
Yoo Jeong Seong
Kyungil Woo
Hyun Joo Yoo

Spain

Coral Garcia Guadix

Switzerland

Laetitia Lehmann

Taiwan

Chih-Yuan Kevin Huang
Ling Luby Lu
Yi Fang Tai

United Arab Emirates

Sameena Sadiq Ali
Rana Barhoush
Muhammad Farooq
Nimendra Lethbridge
Ju Long
Nikhil Vinayakrishnan
Olena Zhuzha

United Kingdom

Haris Ansell
Emilia Makula
Hywel David Joseph Morgan

Nishanth Narendran
Babatunde Adeyeye Ogunwusi
Clare Round
Joseph Tillekeratne

United States

Joyce K. Batterson
Jessica Cruz
Kristina Davis
Kratika Dubey
Valerie Francisco
Frias Luisana
Jennifer R. Gambill
Annah Gohori Mpondi
Yuliang Le
Abraham Leon
Abby Leung-Kibby
Yiming Liu
Ruben Malave
Kristin Ockenfels
Abraham Leon
Abby Leung-Kibby
Yiming Liu
Ruben Malave
Kristin Ockenfels
Christopher M. Orlandini
Nolan Pacchiana
Tiffany Lauren Polyak
Malcolm Rowe
Rachel Sage
Marielle Scholl
Nidhi Kanaiyalal Shah
Madeline J. Stoeri
Justin Storm
Richard J. Torres Jr.
Alesya Vladimirovna Vasilenko
Matthew Waldschmidt
Kevin Watts
Tahiti Weaver
Mukadaisi Wumaier
Shu Yang

Vietnam
Linh Nguyen

Yemen
Mazen Ali Mahyoub Abdu
Maeen Al-Zubery Bazel

PLACE YOUR AD HERE

Be featured in *ACAMS Today* and access a network of over 100,000 anti-financial crime members.

**To advertise in
ACAMS Today
contact:**

**Andrea Winter
1.786.871.3030
awinter@acams.org**



JOIN US IN THE FIGHT AGAINST HUMAN TRAFFICKING

3 FREE VIRTUAL EVENTS

FOLLOW • MONEY



FIGHT • SLAVERY

Co-Creators of the “Expert Analysis of Open Source Material relating to Child Sexual Abuse Material (CSAM) and Sex Trafficking occurring on OnlyFans.com”

DARKWEBATHON: RALLY FOR ACTIONABLE INTELLIGENCE

March 29 - April 3, 2023 (Includes training day and awards)

2 Day Hackathon-Type Challenge with Emerging Technology Training

- Hash Challenge • Email Challenge • Cryptocurrency Challenge •

REGISTER: <https://FollowMoneyFightSlavery.org/darkwebathon-2023/>

ANNUAL SUMMIT

Human Trafficking is a
Financial Crime:
An Industry Call to Action

April 26 - 27, 2023

- Register to Attend -
- Apply to Speak -
- Apply to Sponsor -

Hear from
Industry
Leaders

AML
Cyber Security
Law Enforcement
Cryptocurrency
BSA

REGISTER: <https://FollowMoneyFightSlavery.org/atii-summit-2023/>

TRUST & SAFETY

SYMPOSIUM

9am - Noon EST

April 25, 2023

Online /offline safety training
for children and teens
to safeguard
them from
human trafficking
and exploitation

Students
Academia
Parents

REGISTER: <https://FollowMoneyFightSlavery.org/atii-summit-2023/>