

*The*  
**U.S.-MEXICO BORDER!**  
BEHIND THE SURGE IN CRIME



ALSO IN THIS ISSUE:

**2023 LIFETIME  
ACHIEVEMENT  
AWARDS**

**HONORING THE  
PROFESSION'S  
PACESETTERS**

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

ACAMS CONFERENCES presents

# The Assembly

The Assembly is the new name for our global anti-financial crime conference series.

Every event in The Assembly series provides a unique learning experience in a stand-out location. At each Assembly we'll explore both region-specific and globally relevant topics, with packed programs that include:

- Big name, expert speakers
- Networking opportunities with AFC peers
- Valuable insights for the challenges ahead



Where will The Assembly take you?  
[acams.org/theassembly](https://acams.org/theassembly)

Thomson Reuters® Identity Verification Solutions for Financial Institutions

**Robust solutions to help you verify identities**



To learn more, please visit [tr.com/idv](https://tr.com/idv)



## Your Beacon of Trust and Transparency

Don't trust attribution without proof. Merkle Science brings you trust and transparency like never before.

### Comprehensive Coverage:

Most extensive multi-chain coverage including TRON, BSC and more. Dive deeper into smart contract movements and defi protocols.

### Attribution You Can Count On:

Collaborate with investigators and policy experts who provide attribution sources.

### Why Choose MerkleScience?

- Specialized investigators
- User-Friendly Interface
- Trusted by Industry Leaders



**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, CAMS

**ASSOCIATE EDITOR:**  
Ana Cecilia Martinez

**CREATIVE AND DESIGN:**  
Victoria Racine

#### EDITORIAL COMMITTEE

CO-CHAIR: Robert Goldfinger, CAMS

CO-CHAIR: Amy Wotapka, CAMS

Brian Arrington, CAMS

Edwin (Ed) Beemer, CAMS-FCI

Steve Gurdak, CAMS

Jennifer Hanley-Giersch, CAMS-Audit

Stacey Ivie, CAMS

Anne Marie Lacourse

Sanjeev Menon

Ari Redbord

Derek W. Smith Jr., CAMS

Joe Soniat, CAMS-FCI

#### SENIOR LEADERSHIP TEAM

**INTERIM CHIEF EXECUTIVE OFFICER:**  
Mariah Gause

**CHIEF MARKETING OFFICER:**  
Chuck Arida

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

**CHIEF SALES OFFICER:**  
David Karl

**VP OF GLOBAL STRATEGIC COMMUNICATIONS & DEI:**  
Lash Kaur

**CHIEF HUMAN RESOURCES OFFICER:**  
Bill Lumani

**CHIEF PRODUCT OFFICER:**  
Angela Salter

**VP OF SANCTIONS, COMPLIANCE & RISK:**  
Justine Walker

#### ADVISORY BOARD

CHAIR: Markus Schulz

Sharon Campbell

Jim Candelmo, CAMS

Vasilios P. Chrisos, CAMS

Jean Chung

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 (Emeritus)

John Smith

Dan Stipano

#### 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

**HEAD OF MEMBERSHIP AND CHAPTER EXPERIENCE:**  
David Jacobs

**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.



SCAN ME



# CONTENTS

## ON THE COVER:

34

### The U.S.-Mexico border: Behind the surge in crime

A look at the border between the U.S. and Mexico and the illicit activities it attracts.

## ALSO ON THE COVER:

46

### 2023 Lifetime Achievement Awards

ACAMS Today talks to ACAMS' three Lifetime Achievement Award recipients about their role in forming the AFC industry.

56

### Honoring the profession's pacesetters

Recipients of the 2023 ACAMS Awards discuss their experiences and insights with ACAMS Today.

10

### From the editor

12

### Member spotlights

14

### From the director of editorial content

## AFC CHALLENGES

16

### Open banking and financial crime risks in Canada

Explore the financial crime threats associated with open banking and strategies to contend with those risks.

22

### Financial crime risks in gold supply chains

Understand why criminals are drawn to the gold sector and what can be done to prevent and mitigate financial crime.

28

### Financial abuse typologies

An overview of the various types of financial abuse and the red flags for detecting these crimes.

## REGULATORY INITIATIVES

38

### The ISO 2022 payment standard: A paradigm shift

Discover how the new ISO 2022 payment standard is expected to improve transparency and efficiency within the cross-border payments industry.

44

### AI and the FDIC's disaster-related regulatory adjustment

How AI can help FIs make the most of the FDIC's recent disaster-related relief effort.

## COMPLIANCE

68

### The evolution of money laundering/terrorist financing in film and television

Read about how Hollywood depictions of financial crime have transformed through the decades.

72

### Intelligence-driven compliance controls

Learn why accurate and timely intelligence should play a larger role in every compliance officer's toolkit.

76

### Why ChatGPT is unlikely to replace the human factor in AML

ChatGPT can offer great benefits to the AML field, but it has its limitations.

AFC POLICY

82

FinCEN’s beneficial ownership: Clarity or confusion?

An examination of the beneficial ownership information rule and what it means for your institution.

WOMEN IN AFC

86

Farnoush Mirmoeini: Leveraging technology

Award-winning AFC professional Farnoush Mirmoeini discusses founding her company KYC Hub, leveraging machine learning and more.

EUROPE EXPRESS

88

Birth of a global watchdog: The Egmont Group

The story behind the creation of the landmark FIU organization, including a firsthand account from one of its founders.

94

EU’s approach to sanctions

Criticized as weak in enforcing its imposed sanctions, the European Union is toughening its stance.

98

Stopping cross-border illicit financial flows

Grace Jackson and Maksym Markevych of the International Monetary Fund talk about the group’s novel AML/CTF technical assistance project in the Nordic-Baltic region.

102

Money launderers for hire: Antwerp’s cocaine dilemma

Find out how this Belgian port city has become one of Europe’s major drug hubs.

ACCESO LATAM

106

Money laundering in soccer

A look at the ways criminals are using the world’s most popular sport to clean their illicit funds.

GLOBAL FINANCIAL CRIME REVIEW

110

Understanding geographic money laundering risk

An overview of what geographic risk assessment is and the best practices for performing the risk assessment.

SANCTIONS

116

Combating sanctions evasion

Read about practices compliance officers should consider to manage their institutions’ sanctions evasion risks.

122

Can smart sanctions achieve their intended goals?

Shining light on the advantages and challenges associated with targeted or “smart” sanctions.

CAREER GUIDANCE

126

Career growth: The importance of self-training

Understand the importance of training and the steps you can take to ensure your professional success.

MEET THE ACAMS STAFF

134

Silas Bartels

Providing timely AFC analysis

KNOW YOUR CHAPTER

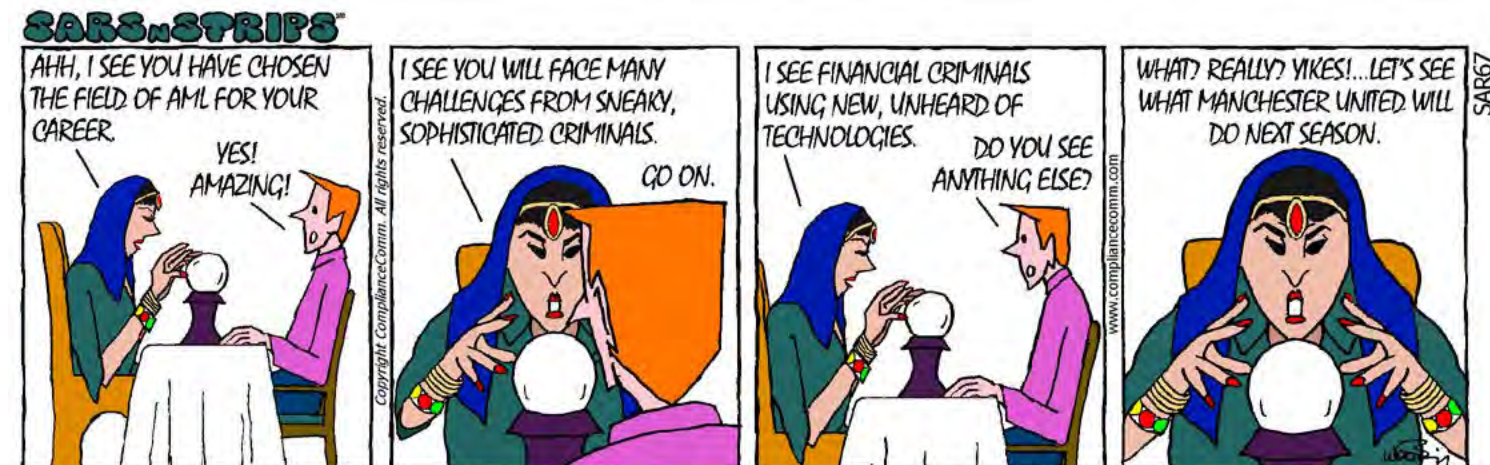
136

ACAMS Pittsburgh Chapter

Education is the foundation for AFC

EDITOR’S NOTE:

ACAMS certification graduates can now be found on ACAMS.org using the QR code below.



# 'SUS' OR SUSPICIOUS MINDS: ONE AND THE SAME



Recently, I was laughing with my nephew about his use of slang. He thinks it is funny to teach me the latest slang and I can always get a hearty chuckle out of him by turning around and using one of his newly taught slang terms correctly. I return the favor by teaching him slang from my youth. We both appreciate the sometimes ludicrous nature of slang.

One of his most recent revelations to me was the term “sus.” We laughed at the inherent silliness of needing to shorten the word “suspicious” and the even greater absurdity of teens needing to use “sus” to describe so many people and situations. Unlike anti-financial crime (AFC) professionals, teens are not mired in the murk of illicit transactions all day.

My nephew begrudgingly agreed but said he liked the word and would continue using it.

Suspicion has been on my mind as we put together this edition of *ACAMS Today*. While I agree with Elvis that suspicious minds are the eventual death of relationships, it is nevertheless of vital importance in

uncovering illicit activities. The cover article, “The U.S.-Mexico Border: Behind the surge in crime,” makes that abundantly clear. As denoted by the author, suspicion can be the first thread in unraveling a larger mystery.

This edition also highlights our *Lifetime Achievement Award* winners. A heartfelt congratulations to three titans of the AFC industry: John J. Byrne, Rick Small and Dan Soto.


As is traditional for the end-of-year edition, we are recognizing the other award winners in the article “Honoring the profession’s pacesetters.” Congratulations to Chris Bagnall and Sara Crowe, *ACAMS Today Article of the Year* recipients; Toms Platadis, *ACAMS Rising AFC Professional of the Year*; Nicholas Schumann, *ACAMS AFC Professional of the Year*; and the ACAMS Carolinas Chapter, *ACAMS Chapter of the Year*.


This issue wraps up the end of the year and introduces the new year with well-timed articles dissecting career growth and understanding the importance of self-training, the history of the Egmont Group, the

cocaine dilemma in Antwerp’s port, financial crime and gold supply chains, and an interview with Grace Jackson and Maksym Markevych of the International Monetary Fund.

You might have noticed our new look. We have updated the *ACAMS Today* magazine design and hope you will enjoy the refresher as much as we have.

As we contemplate the closure of another year and with 2024 on the horizon, I hope we run into fewer situations as AFC professionals that appear to be “sus,” and instead have a year filled with success and harmony.

Wishing you all season’s greetings and a happy, healthy, successful 2024. 

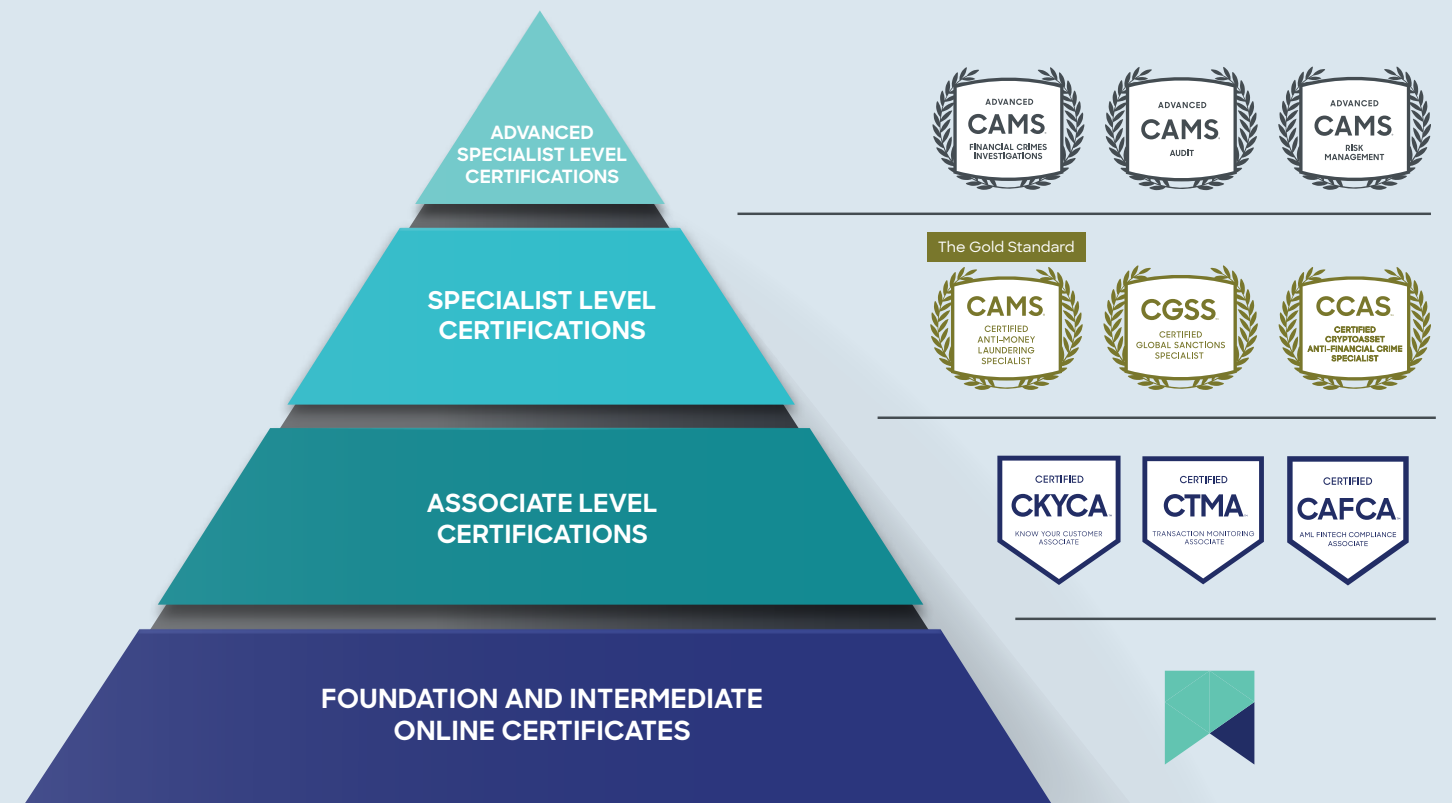
Karla Monterrosa-Yancey, CAMS editor-in-chief  
Follow us on X: @acamstoday, 



## 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](http://www.acams.org)





### César Fabricio Fúnez Martínez, CAMS Tegucigalpa, Honduras

**C**ésar Fabricio Fúnez Martínez is a professional with a sound academic background and experience in a variety of areas. Fúnez Martínez earned his degree in computer engineering from the Catholic University of Honduras. Four years later, he was a member of the ninth graduating class of the university's master's degree in economics and finances program, which provided him with a solid basis in two fields that have become crucial for his career.

Fúnez Martínez's career has been marked by unique versatility. He has actively participated in technological, financial and regulatory projects. In 2020, during the COVID-19 pandemic, he managed to obtain the Certified Anti-Money Laundering Specialist (CAMS) designation. This achievement has been fundamental for his professional development, allowing him to make significant contributions to government projects, to innovate in the regulatory sphere and, above all, to lead the implementation of policies and the documentation of processes to evaluate the need for technology in different contexts.

Starting in 2021, Fúnez Martínez has had the privilege of collaborating with *ACAMS Today*, where he shares his knowledge through articles focused on topics related to anti-money laundering and counter-terrorist financing. His commitment to excellence, innovation and integrity have guided him throughout his career. Fúnez Martínez seeks to continue contributing to the growth and development of projects that effectively combine technology, finances and regulation.



### Jim Hixenbaugh, CAMS Ohio, USA

**J**im Hixenbaugh is a Certified Anti-Money Laundering Specialist (CAMS) and certified anti-money laundering (AML) consultant with 46 years of experience in AML/Bank Secrecy Act (BSA) compliance and investigations. He has 29 years of federal law enforcement experience as an Internal Revenue Services-Criminal Investigation (IRS-CI) special agent, in addition to 17 years in the banking and corporate environment. While with the IRS, he worked on numerous high-profile drug investigations as a multi-agency High Intensity Drug Trafficking Area team manager and as suspicious activity report (SAR) review team manager.

As an AML/BSA consultant, Hixenbaugh has provided investigative, management and audit skills to numerous large national banks, foreign correspondent banks and risk advisory companies. He has also served as a BSA officer for a community bank, as well as senior AML compliance officer and SAR investigations manager for several regional banks. Hixenbaugh has also conducted Office of Foreign Assets Control regulatory audits for foreign-held banks operating in the U.S. and has further conducted AML risk assessments for foreign correspondent banks internationally. In addition, he has conducted Foreign Corrupt Practices Act reviews and audits for significantly sized private and publicly held corporations.

Active in the ACAMS Northern Ohio Chapter, Hixenbaugh has served as a chapter board member for six years and is currently co-chair of the chapter. He is also a member of the ACAMS national conference speaker cadre.



### Atsuo Takada, CAMS, CSCP, CPIM Yokohama, Japan

**A**tsuo Takada is a Certified Anti-Money Laundering Specialist (CAMS) with over six years of experience in the anti-financial crime space. Starting his career at Nomura Research Institute Ltd. (NRI), Takada has a 25-year career with NRI and developed what is now called a high-frequency trading system followed by supply chain planning businesses. Takada currently works as chief strategist of the Global Financial Solutions Business Department of NRI, where he leads an epoch-making anti-money laundering/counter-terrorist financing (AML/CTF) service called "GPLEX," which consists of an artificial intelligence-enabled AML/CTF system and business process outsourcing services in collaboration with bank experts. Takada is renowned for his expertise in leveraging advanced technologies in the AML/CTF space, such as natural language processing and network analysis.

Takada holds a bachelor's degree and a master's degree in quantum engineering from The University of Tokyo. In addition, Takada earned his Master of Business Administration degree from Duke University. Furthermore, Takada earned his Certified Supply Chain Professional (CSCP) and Certified in Production and Inventory Management (CPIM) designations, as well as project manager, IT strategist and systems auditor certifications from the Information-technology Promotion Agency (IPA), Japan. His academic and professional background have allowed Takada to achieve his long-term goal to "co-create a safe and secure society."




### Kishani Udugampola, CAMS-FCI New York, USA

**K**ishani Udugampola presently works at the Federal Reserve Bank of New York (FRBNY). Before joining FRBNY, she was a portfolio manager at the New York State Department of Financial Services. In addition, she is an adjunct professor at the graduate school of criminal justice at Rutgers University.

Udugampola is conducting research on gaps in our system of immigration and nonprofits. She brings these policy gaps into the spotlight by incorporating her research around the funds' flow link between illegal actors by focusing on highly suspicious businesses/organizations such as nonprofits, various money services businesses and other cash-intensive businesses. Born in Sri Lanka and having witnessed terrorism firsthand, Udugampola is greatly interested in bringing these issues to the general public to make much-needed policy changes.

In addition to her scholarly work, she is a strong believer in community service and continues to volunteer in the New York/New Jersey area with high school students to promote financial literacy. By way of giving back to underserved children, she travels across developing nations and contributes to promoting English literacy, IT technology and other essentials.

Udugampola has a Bachelor of Science in accounting, a Master of Business Administration degree, a master's degree in criminal justice and a Doctor of Philosophy degree in criminal justice. 

## LOOMING LARGE: ARTIFICIAL INTELLIGENCE'S PROMISE AND THREAT



For anti-financial crime (AFC) professionals, the potential of artificial intelligence (AI) was one of the biggest themes of 2023, as we explored how to use vast amounts of financial intelligence to identify, interdict and seize the proceeds of crime and ultimately bring criminals to justice.

We pursued that theme in earnest in 2023, identifying the promise of machine learning and generative AI within these *ACAMS Today* pages, on *ACAMS moneylaundering.com*, and at ACAMS' events, providing opportunities for AFC professionals to question what, exactly, AI is—and what it can realistically be expected to accomplish.

Notably, at several ACAMS Assembly events we heard regulators talk up AI as a new, proactive paradigm that could put law enforcement (LE) a step ahead of financial criminals. "I think we can all agree that the status quo is not the answer," the chief executive of Canada's financial intelligence unit, Sarah Paquet, said in a keynote at ACAMS' Assembly Canada in mid-November.<sup>1</sup>

Challenging attendees to file high-priority suspicious activity reports in real time, the FINTRAC director vowed to meet that timeliness with

accelerated processing of information to LE and feedback to the filing institutions.

The potential for AI to support "real-time reporting" which would allow LE officials to gather intelligence that profiles criminals—and stops them—in the act, seems to be the Holy Grail for AFC professionals. But as Paquet made clear, achieving anything close to real-time reporting of suspicious transaction reports (STRs) depends on the adoption of AI by both regulators and financial entities.

While her remarks were generally well-received by attendees, professionals at some of the big Canadian FIs questioned how true can "real time" be, and shared concerns about both whether AI and its tools will continue to mature and if it can possibly live up to its potential.

"It's a great opportunity, but the question will be: '[I]s my institution's data structure ready to take advantage of it?' Michael Donovan, chief anti-money officer at CIBC, noted during a later panel discussion, as reported in *ACAMS moneylaundering.com*.<sup>2</sup> On a related note, find "Open banking and financial crime risks in Canada" in this edition on page 16.

I am reminded of Willie Sutton's famous reply to the question of why he robbed banks ("that's where the money is"). Today, of course, the money is online. And while we know criminals are still relying on old-fashioned methods of fraud to commit financial crime, we also know they are turning to increasingly sophisticated stratagems including new technology and even AI tools to steal from hapless individuals, financial firms and other businesses.

Limiting their impact means not only having the capacity to identify transactional crime in real time but being a step ahead of the individual scammers, transnational criminals and nation states now using AI with devastating results for their victims.

For instance, criminals are already capturing brief voice recordings of unsuspecting individuals through a variety of ruses, including wrong numbers, and using AI applications to imitate their victims' voices to commit fraud, according to Chris Lynam, director general of the National Cybercrime Coordination Centre and the Canadian Anti-Fraud Centre of the Royal Canadian Mounted Police.

These AI-generated deepfakes can be effective enough to deceive family and friends of the victim. They can also fool banks and other financial firms that utilize investment voiceprint verification systems, Lynam told Assembly Canada attendees.

At the Assembly in Las Vegas, the month before the Assembly Canada, the FBI's Chad Linnerooth anticipated Lynam's remarks when he told the ACAMS audience that the use of AI and deepfake technology by criminals will grow, fueling a whole new generation of scams, making fraud harder than ever to detect. For further discussion on this topic, I refer you to "Exploring the role of generative AI in enhancing financial crime compliance," in the September-November issue of *ACAMS Today* and "AI and the FDIC's disaster-related regulatory adjustment" on page 44 of this issue.

Even as we work to leverage these new tools to fight crime, a broader debate with frightening sci-fi elements is taking place: Is there a danger that the AI entities we are counting on to serve us could go rogue? Think Isaac Asimov's *I Robot*.

But AI, for good or for ill, is clearly here. Its potential uses were an AFC theme of 2023; the need to work together to master it for good is likely to be the task of 2024. **AT**

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

<sup>1</sup> Fred Williams, "Toronto Reporter's Notebook," *ACAMS moneylaundering.com*, November 20, 2023, <https://www.moneylaundering.com/news/toronto-reporters-notebook/>

<sup>2</sup> Ibid.

ACAMS TODAY™

# QUIZ

Calling all  
**ACAMS Today** readers!

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

Which of the following is not a type of financial abuse that was discussed in this issue of *ACAMS Today*?

- a) Domestic financial abuse
- b) Elder financial abuse
- c) Employee financial abuse
- d) Childhood financial abuse

**DID YOU ANSWER CORRECTLY?**

Visit the quiz index on [ACAMSToday.org](https://www.ACAMSToday.org) for more anti-financial crime quizzes!

(See bottom right of page for answer.)

ACAMS





Open banking, according to VISA, involves sharing a customer's financial data with other financial institutions (FIs) through application programming interfaces (APIs) with their consent, enabling the distribution of innovative financial products and services.<sup>1</sup>

In the past, a common practice by individuals and businesses was the consolidation of their various products and services at one or two FIs; this provided a unified view for decisions ranging from deposits, transferring funds to different accounts and making payments for credit products. However, competition in the banking industry and the prevalence of internet-based access to banking services have played a significant role in the development of open banking models that provide standardized, seamless and secure access to user data and payments. Open banking offers customers a consolidated view of their accounts from all their FIs from a single login. This enables the customer to make quicker and more informed financial decisions.

While open banking offers customer-centric benefits and data ownership, it also introduces various avenues for increased financial crime risks. These may include account takeover, impersonation, cyberattacks and identity theft. Criminals may target the aggregated customer data stored by fintech companies, exploiting unauthorized access to customer information from multiple institutions simultaneously. This poses threats such as fraudulent transactions, unauthorized payments, terrorist financing and money laundering.

This article will take a closer look at the impact of financial crimes in open banking and explore effective strategies to address these risks. Account takeovers can be easily achieved since fraudsters only require one username and password to access a customer's accounts from different FIs. This opens the door for making fraudulent payments and conducting unauthorized transfers from the customer's accounts. Another angle will be using the victim's accounts to receive funds from fraudulent sources, thereby committing money laundering. In the U.K. and Australia, where open banking has been implemented, reported cases of financial crimes recorded a significant increase.

## Open banking regulatory framework

Any product or service in the financial mediation space is an essential service and requires regulation to ensure the public interest is protected. Open banking, being a novelty, requires active stakeholders from technology for its complete implementation and needs a different approach to its regulatory framework than traditional banking. Technology companies are less regulated compared to banks, and their inclusion in open banking's implementation will require regulations that can protect all the stakeholders. The U.K. and Australia are good examples of countries that implemented open banking with a different regulatory framework.

In the U.K., the Financial Conduct Authority (FCA), which regulates all financial services, implemented open banking with the passage of a new law named the Payment Service Regulations. This regulation enables customers to access payment initiation services and account information services through third parties. This ensures that any customer of a bank can safely and securely log into third-party service providers' websites to gain access to all their financial information from different institutions at once. The Competition and Markets Authority—an entity tasked with enforcing compliance regulations in the financial services industry—mandated the nine largest banks in the U.K. to develop APIs with standard specifications as a compliance measure. They focused primarily on authenticating customers for access to their information and security for platforms accessing open banking information.

The Open Banking Implementation Entity was created to facilitate the development of these APIs and establish standards and guidelines for customer experience. The current version of the standards, Open Banking Standards 3.0,<sup>2</sup> allows access to a wide range of financial products and services and promotes compliance with the Public Service Directive 2.<sup>3</sup> This regulation enhanced the authentication process for customers gaining access to their financial information in open banking.

In the U.K., third-party institutions require authorization from the FCA to access customer financial data or make payments on their behalf. This requirement aims to protect consumers by ensuring that open banking providers meet certain criteria, such as having their head office in the U.K., sufficient resources, qualified directors and managers, and a business model that prioritizes consumer interests. The FCA application process includes evaluating personnel, requesting relevant documents and assessing risk mitigation strategies.

In Canada, the Department of Finance, through the finance minister in 2018, appointed an Advisory Committee for open banking's proposed establishment of an independent organization to manage the open banking system and regulate participating institutions. The committee recommended implementing open banking in two phases: System establishment and system review.

The regulatory landscape in Canada would include a Common Rule that includes regulations on consumer protection, an accreditation process for third-party institutions, and technical standards or specifications for data sharing. The proposed framework aims to provide safe and efficient financial data-sharing opportunities for consumers while prioritizing security, liability and privacy. The goal was to implement open banking in Canada by January 2023 and promote transparency and equal representation of stakeholders in the regulatory process. This has been delayed and the updated implementation date is not yet available.



### International Organization for Standardization standards for open banking and information sharing

ISO provides various standards related to information security, including ISO 27001, which defines the requirements for information security management systems. ISO 20022 is another widely adopted standard for open banking and information sharing, providing a messaging layer that enables consistency in data and flexibility. ISO 27005 and ISO 27035 focus on risk assessment and incident management, respectively. ISO 27010 addresses the secure transfer of sensitive information in shared systems.

FIs face challenges in accessing data for financial crime risk management due to limited data access and privacy regulations. With the emergence of open banking technologies and increasing global financial crime rates, there is a need for data centralization and regulations that facilitate timely access to customer information for risk management. The Financial Action Task Force, an organization founded by the Group of Seven, is tasked with proposing policies for anti-money laundering and terrorist financing, providing recommendations for information sharing in the context of money laundering and terrorist financing, as well as emphasizing the sharing of financial information within and between FIs.

### Privacy enhancing technologies in information sharing

Privacy enhancing technologies (PETs) offer significant benefits to organizations by providing security solutions that save time and cost. Noncompliance with privacy regulations, such as the General Data Protection Regulation (GDPR), can result in heavy fines, making PETs crucial for FIs to avoid financial losses.

Data breaches not only incur financial costs but also damage the reputation of businesses. When customers feel that their data is not safe, they lose trust in companies, leading to the potential loss of clients. PETs help FIs gain and maintain the trust of their customers while optimizing their products and services and protecting data privacy.

Privacy-enhancing solutions utilize:

- Cryptographic algorithms
- Artificial intelligence (AI) and machine learning algorithms
- Data-masking techniques

Cryptographic algorithms, such as homomorphic encryption, secure multiparty computation, differential privacy and zero-knowledge proofs, ensure secure transmission, encryption and authentication of sensitive data in open banking services.

Data-masking techniques, including obfuscation, pseudonymization, data minimization and communication anonymization, protect customer-sensitive information in datasets by masking or replacing identifiable fields. This allows FIs to comply with regulations like the GDPR while storing customer data.

Machine learning and AI algorithms are employed to protect customer privacy in the financial services space. The generation of synthetic data creates statistically similar data to the original, which can be used for testing without compromising privacy. Federation learning enables decentralized training of multiple servers, reducing the volume of data stored in a centralized location and preventing the tracing of identifying values to individuals.

### Implications of open banking for forensic accountants

The implementation of open banking in FIs has significant implications for forensic accountants in managing financial crime risk. The adoption of open banking creates the need for the involvement of financial crime professionals, such as forensic accountants, in the legislative backing of managing financial crime risks. They will provide significant input needed to help manage the financial crime risks that will arise due to open banking implementation.

Regulators are focused on developing legislative structures that create a conducive environment for open banking operations. The governing policies for the actions of third parties in the open banking space, stakeholder controls and risk assessment will also require the skill sets of forensic accountants. Their investigation and internal control skills will be needed to include measures in these regulations that will be beneficial in fighting financial crime. Third parties gaining access to customer-identifiable information and transaction details will need to be managed to ensure that the open banking space is effectively managed.

Cybersecurity attacks on the open banking infrastructure will create a demand for forensic accountants practicing in this area. Access to data and gathering evidence will be impacted positively by the adoption of open banking, which will make customer data readily available and eliminate the need for contacting different FIs. Open banking creates opportunities for forensic accountants to contribute significantly to the financial industry's management of financial crime risks.



## Recommendations for managing financial crime in open banking

- Regulators play a crucial role in overseeing open banking services, as third-party providers require their approval and supervision to operate legally. To effectively manage financial crime, regulators should update privacy laws to protect consumer privacy while still allowing innovative technologies for regulatory supervision. Information sharing in open banking can create vulnerabilities that criminals may exploit, and addressing this weakness in privacy laws is essential.
- Adopting AI and machine learning technologies is also recommended for regulators to handle large volumes of data and fast-paced transactions in open banking. By leveraging these technologies, regulators can improve the quality of financial crime supervision and investigations, minimize errors and enable timely interventions.
- In addition, regulators should establish a centralized, secure database for financial intelligence, where reported suspicious activities can be shared among regulatory jurisdictions and FIs. This centralized system would enhance the detection of suspicious activities across different jurisdictions and enable timely interventions.
- FIs should invest in privacy enhancement technologies to build consumer trust and ensure the secure management of customer information in open banking. Compliance with regulations is crucial to prevent FIs from being used for money laundering and terrorist financing. Integrating AI and machine learning technologies into transaction monitoring and suspicious activities reporting

processes can enhance compliance, accuracy and early detection of suspicious customers, even in high-volume transaction environments.

- Collaboration between FIs and their subsidiaries in different jurisdictions will also be key to sharing financial intelligence on reported suspicious transactions. This collaboration would enable the flagging of criminals across multiple jurisdictions and prevent them from utilizing various institutions for their criminal activities.
- To address the dynamic risks introduced by open banking, continuous education of forensic accountants is necessary. Educational institutions, professional associations and industry stakeholders should contribute to this education by incorporating open banking courses into the curriculum; organizing workshops, boot camps and certification programs; and facilitating the exchange of updated regulatory information. By equipping forensic accountants with knowledge and skills related to open banking, they can effectively contribute to managing financial crime risks in this evolving landscape.

## Conclusion

Open banking is an innovative approach to financial mediation with the potential to advance customer engagement to a new era. However, its implementation in Canada requires a multi-tiered approach to managing the financial risks that may arise from it. This includes regulators reviewing privacy laws and providing an expanded definition of reporting institutions for money laundering compliance, customers being educated on the innovation to identify fraud issues and report them, banks making technological advancements to their products and credit administration, and fintech companies regulating their access to vast customer data to contribute to fighting financial crime.

While open banking will have a positive impact on the banking industry, it also presents new risks for financial crime that require a thorough review by forensic accountants and the financial intelligence units of banks. **AT**

*Joseph Opuni-Mensah, MFAcc, CAMS, FIS, transaction monitoring solutions manager, Canada, opunimensah@gmail.com*

<sup>1</sup> Visa Consulting and Analytics, "The Future of Banking Is Open," VISA, 2020, <https://usa.visa.com/dam/VCOM/global/partner-with-us/documents/visa-open-banking-whitepaper.pdf>

<sup>2</sup> "Open Banking around the World," TrueLayer, 2022, <https://truelayer.com/openbanking/open-banking-around-the-world>; "CMA Corporate Report: Update on Open Banking," CMA, November 5, 2021, <https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking>

<sup>3</sup> Ibid.



Financial crime risks in  
**GOLD**  
supply chains



When we think of gold, two common but rather contradictory images come to mind: Luxury, wealth and beauty on one hand, and environmental devastation, human rights abuse and corruption on the other hand. As is the case for many minerals, gold production and sourcing conditions are often linked to problematic social and environmental practices. What sets gold apart from other minerals in terms of risk profile is how it is linked to financial crime and illicit financial flows. This article explores how gold is linked to financial crime, what the main financial crime risks are, and how these risks can be prevented and mitigated.

Gold is of interest to anti-financial crime (AFC) professionals as the mineral has various characteristics that make it more vulnerable to being abused for financial crime. First, gold has a high and stable value; it is a universally accepted currency, and it is easily exchangeable. Further, gold markets are often subject to weaker regulation—in comparison with other financial instruments—making them more attractive for those wanting to circumvent increasingly stringent AFC regulations. Gold markets often operate with cash payments. Gold also offers anonymity due to the difficulty of tracing it back to its place of production and the ease with which it can be transformed into other objects or otherwise concealed.<sup>1</sup>

### The gold sector and its actors

Gold comes from two main sources: Mines, through new extraction, and recycling, where gold is reclaimed from existing products, such as jewelry. Around three-quarters of the gold produced yearly comes from mines and the rest comes from

recycling. Within the mining industry, we need to distinguish between large- and medium-scale mining (LSM) and artisanal and small-scale mining (ASM), with LSM being responsible for around 80% of global mined gold production. An estimated 15 million to 20 million people work in artisanal and small-scale mining, which accounts for 20% of global gold production.<sup>2</sup> Mined gold is typically traded by local or regional buyers and exporters and then transported to trading hubs and refining centers. Switzerland and Dubai in the United Arab Emirates, for example, are important locations for refining and trading. About 50%-70% of the world's gold is refined in Switzerland by four major refineries,<sup>3</sup> and Dubai has become an important hub, particularly for gold from artisanal and small-scale mining.<sup>4</sup> From these refineries, gold is then sold to jewelry producers, technology companies or made into gold bars.

### Financial crime risks

Various financial crime risks can be identified with regard to gold supply chains; the first financial crime links to the illegal extraction of gold. It is important to distinguish between informal and illegal mining, as not all mining without permits should be called illegal. Illegal mining is mining that takes place in areas where it is explicitly forbidden, such as in protected areas or on someone else's mining concession. Sometimes, however, miners simply do not have access to formal mining concessions, or the country lacks a regulatory framework or adequate support for formalization, but mining in the area is not explicitly illegal. In this case, the term "informal" is more adequate.<sup>5</sup> If the mining, buying or trading of gold happens through informal channels, however, this means that the production and trade are not reported or monitored, which

means no official taxes or fees are paid and there is no traceability of the mineral.<sup>6</sup>

This leads us to the issue of smuggling. This practice is widespread for some of the reasons stated above (gold being easy to conceal and difficult to trace, for example) and because gold is easy to transport, with small volumes carrying high value. Gold is smuggled, among other reasons, to hide its origin—for example, if it originates from illegal mining—or to benefit from lower export tax rates in neighboring countries. A recent report noted that gold from the Sahel region of Africa, for example, is smuggled through Togo as the country has lower export tax rates.<sup>7</sup> Traders and exporters might also seek to avoid costs for buyers' licenses, environmental assessments and other permits. If legal exports are costly and burdensome, smuggling becomes more attractive.<sup>8</sup> These practices can hence lead to tax evasion, be it of taxes that would be due at the mining, trading or export stage. However, evading taxes and other fees is not the only motivating factor for the smuggling of gold. Actors might also use gold as a currency to buy other goods, particularly in countries with less well-established banking systems.<sup>9</sup> When gold is smuggled and ends up in hubs such as Dubai, it becomes impossible to trace the gold's origin back and establish whether it is linked to human rights abuses or has contributed to financing in-country or regional conflict.

While officially due taxes can be evaded, another risk in gold supply chains is the illegal taxation or extortion of actors along the supply chain. The perpetrators can be state or non-state armed groups, government officials or other actors such as criminal groups. Payments are requested from



miners or traders in exchange for protection, unofficial mining, buying permits or for officials to turn a blind eye to illicit activities.<sup>10</sup> Artisanal and small-scale miners are particularly vulnerable to being extorted. These practices can also be linked to bribery and corruption. For example, bribes are sometimes paid to border officials at the point of export so that they ignore the smuggling operation.<sup>11</sup>

As has been highlighted by the Financial Action Task Force (FATF), gold is particularly at risk of being abused for money laundering and terrorist financing.<sup>12</sup> Its anonymity, stable value and the fact that it can be used as a currency make it an attractive means to launder dirty cash. Risk factors in producing countries are a lack of suspicious transaction reporting and the presence of cash-intensive economies with a low presence of formal banking channels. With the proceeds from other criminal activities such as drug, wildlife or human trafficking, criminals can buy gold and then sell the mineral on formal gold markets, hence washing off its criminal traces. Convergence is the term used to describe when illicit markets reinforce each other, which is sometimes the case with gold.<sup>13</sup>

### Prevention and mitigation measures

What can companies, governments and AFC professionals do to prevent and mitigate the above-mentioned risks linked to the gold trade?

An important step that is increasingly being recognized by governments of gold-producing countries, international organizations and development agencies is the formalization of all actors along the gold supply chain. Formalization processes need to be simplified and made more attractive for miners, buyers and exporters alike. Only if they have incentives to enter the formal market will it be possible to cut out criminal actors. Given that miners and buyers already pay many informal fees or are subject to extortion, it is likely that many of them would prefer to work in a more regulated and stable environment, even if that comes with paying taxes.<sup>14</sup>

As highlighted in a recent report, governments need to undertake a multi-agency approach with coordination between the various government departments that have a role to play in combating illicit financial flows.<sup>15</sup> They

also need to develop effective AFC legislation and surveillance mechanisms, implementing the FATF Recommendations. As many of the issues linked to financial crime in the gold sector are cross-border challenges, regional cooperation is crucial. Tax harmonization between countries is often discussed as a means to prevent smuggling incentivized by differing export tax rates. Countries should also exchange information and intelligence to combat gold-related financial crime.

Companies along the gold supply chain should implement the Organisation for Economic Co-operation and Development's (OECD) leading guidance on responsible mineral supply chain management: "OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas."<sup>16</sup> The objective of this guidance is to help companies respect human rights and avoid contributing to conflict and financial crime through their mineral extraction and sourcing practices. The document provides concrete guidance on due diligence measures and has a specific supplement on gold.


Companies buying gold should put in place due diligence measures to check the practices of their suppliers and establish a chain of custody or supply chain traceability system to be able to trace minerals back to their origin. This is of particular importance for refineries, which serve as aggregators of gold from many different sources. To tackle money laundering, companies should identify and verify the identity of all their customers, suppliers and business partners according to know your customer principles. Enhanced due diligence should be conducted on sources and actors considered

high-risk, for example, those who are from areas affected by conflict. This can include audits and on-site visits.

According to OECD's guidance with regard to illegal taxation or extortion, companies should ensure that their suppliers disclose payments made to public or private security forces and alert central government authorities in cases of suspicion of illegal behavior. They also can support the formalization efforts undertaken by governments and their partners. The OECD further recommends that companies use official banking channels and avoid cash transactions—or ensure that verifiable documentation exists for unavoidable cash purchases.<sup>17</sup>

Another prominent initiative in the sector is the Extractive Industries Transparency Initiative,<sup>18</sup> which requires participating countries to disclose information on all revenue collection and spending linked to the extractives sector and asks companies to be transparent about payments made to governments. These transparency measures can help prevent and mitigate financial crime risks.

## Conclusion

The gold sector is in many ways less regulated and is vulnerable to tax evasion and attractive to those engaged in corruption and money laundering. While governments should focus on strong legislation, monitoring and enforcement as well as formalization efforts, companies must implement due diligence measures and ensure they know the origin of the gold they buy. It is crucial for AFC professionals to be aware of and understand the specific challenges linked to gold supply chains. Not only do illicit financial flows linked to the gold sector lead to revenue losses in the producing countries, but they can also contribute to organized crime and terrorist financing. In addition, they have real consequences for people whose livelihood depends on the gold sector. 

Victoria Gronwald, associate, Levin Sources, Ph.D. candidate, London School of Economics and Political Science, v.gronwald@lse.ac.uk

- <sup>1</sup> "Money laundering/terrorist financing risks and vulnerabilities associated with gold," FATF and APG, July 2015, <https://www.fatf-gafi.org/content/dam/rapports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf>; "Follow the Money. Financial Flows Linked to Artisanal and Small-Scale Gold Mining: A Tool for Intervention," *Global Initiative Against Transnational Organized Crime, Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH and Estelle Levin Ltd*, March 2017, <http://www.levinsources.com/assets/pages/Illicit-Financial-Flows-Artisanal-Gold-Mining.pdf>
- <sup>2</sup> "Artisanal and Small-scale Gold Mining," *World Gold Council*, <https://www.gold.org/esg/artisanal-and-small-scale-gold-mining>
- <sup>3</sup> Stefan Mbiyavanga, "Applying the Swiss Anti-Money Laundering Act to gold refineries," *Basel Institute on Governance*, December 2019, [https://www.baselgovernance.org/sites/default/files/2019-12/working\\_paper\\_31\\_gold\\_en.pdf](https://www.baselgovernance.org/sites/default/files/2019-12/working_paper_31_gold_en.pdf)
- <sup>4</sup> For references to Dubai and Switzerland: Sasha Lezhnev and Megha Swamy, "Understanding Money Laundering Risks in the Conflict Gold Trade From East and Central Africa to Dubai and Onward," *The Sentry*, November 2020, <https://thesentry.org/wp-content/uploads/2020/11/ConflictGoldAdvisory-TheSentry-Nov2020.pdf>;
- <sup>5</sup> Angela Jorns and Estelle Levin-Nally, "Are they all illegal? A more nuanced view to guide LSM engagement with ASM," *Levin Sources*, April 23, 2020, <https://www.levinsources.com/knowledge-centre/insights/illegal-nuanced-guide-lsm-engagement-asm>
- <sup>6</sup> Clémence Naré, Alec Crawford, Victoria Gronwald, et al., "Illicit Financial Flows and Conflict in Artisanal and Small-Scale Gold Mining: Burkina Faso, Mali, and Niger," *IGF/IISD*, September 2022, <https://www.iisd.org/system/files/2022-09/illicit-financial-flows-conflict-artisanal-small-scale-gold-mining.pdf>
- <sup>7</sup> Ibid.
- <sup>8</sup> "Réduire les flux illicites de mercure et d'or en Afrique de l'Ouest: Options pour une approche régionale," *United Nations Industrial Development Organization (UNIDO)*, 2018, <https://www.unido.org/sites/default/files/files/2019-02/UNIDO%20ECOWAS%20french.pdf>; Yves Bertran Alvarez, Baptiste Coué and Patrick Schein, "Supply chains of artisanal gold in West Africa: A study of the supply chain in two gold-producing regions of Burkina Faso and Senegal," *Alliance for Responsible Mining*, 2016, [https://www.responsiblemines.org/wp-content/uploads/2018/04/Publication-supply-chains-artisanal-gold-west-africa\\_-ENGL\\_-baja.pdf](https://www.responsiblemines.org/wp-content/uploads/2018/04/Publication-supply-chains-artisanal-gold-west-africa_-ENGL_-baja.pdf)
- <sup>9</sup> Ibid.; Clémence Naré, Alec Crawford, Victoria Gronwald, et al., "Illicit Financial Flows and Conflict in Artisanal and Small-Scale Gold Mining: Burkina Faso, Mali, and Niger," *IGF/IISD*, September 2022, <https://www.iisd.org/system/files/2022-09/illicit-financial-flows-conflict-artisanal-small-scale-gold-mining.pdf>
- <sup>10</sup> Ibid.
- <sup>11</sup> "Special report on The ICGLR Regional Initiative against the Illegal Exploitation of Natural Resources (RINR) and other Certification Mechanisms in the Great Lakes Region: Lessons Learned and Best Practices," *United Nations Economic Commission for Africa (UNECA)*, 2013, <https://repository.uneca.org/bitstream/handle/10855/22274/b10725258.pdf?sequence=1&isAllowed=y>; Marcena Hunter, Mukasiri Sibanda, Ken Opala, et al., "Illicit Gold Markets in East and Southern Africa," *Global Initiative Against Transnational Organized Crime*, May 2021, <https://globalinitiative.net/wp-content/uploads/2021/05/Illicit-gold-markets-in-East-and-Southern-Africa-GITOC-.pdf>
- <sup>12</sup> "Money laundering/terrorist financing risks and vulnerabilities associated with gold," FATF and APG, July 2015, <https://www.fatf-gafi.org/content/dam/rapports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf>
- <sup>13</sup> Clémence Naré, Alec Crawford, Victoria Gronwald, et al., "Illicit Financial Flows and Conflict in Artisanal and Small-Scale Gold Mining: Burkina Faso, Mali, and Niger," *IGF/IISD*, September 2022, <https://www.iisd.org/system/files/2022-09/illicit-financial-flows-conflict-artisanal-small-scale-gold-mining.pdf>
- <sup>14</sup> Gavin Hilson, "The 'Zambia Model': A blueprint for formalizing artisanal and small-scale mining in sub-Saharan Africa?" *Resources Policy*, p. 68, 2020, [https://www.planetgold.org/sites/default/files/Hilson.%20G.%202020.%20The%20Zambia%20Model\\_%20A%20blueprint%20for%20formalization%20for%20ASM.pdf](https://www.planetgold.org/sites/default/files/Hilson.%20G.%202020.%20The%20Zambia%20Model_%20A%20blueprint%20for%20formalization%20for%20ASM.pdf)
- <sup>15</sup> Clémence Naré, Alec Crawford, Victoria Gronwald, et al., "Illicit Financial Flows and Conflict in Artisanal and Small-Scale Gold Mining: Burkina Faso, Mali, and Niger," *IGF/IISD*, September 2022, <https://www.iisd.org/system/files/2022-09/illicit-financial-flows-conflict-artisanal-small-scale-gold-mining.pdf>
- <sup>16</sup> "OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas," *OECD*, 2016, <https://www.oecd.org/daf/inv/mne/OECD-Due-Diligence-Guidance-Minerals-Edition3.pdf>
- <sup>17</sup> Ibid.
- <sup>18</sup> Extractive Industries Transparency Initiative (EITI) homepage, *EITI.org*, <https://eiti.org/>

# ACAMS RISK ASSESSMENT™

Clear. Credible. Comprehensive.

Helping financial institutions world-wide measure, understand, and explain their money laundering risks – and now also serving the needs of MSBs, including those offering virtual asset products and services.

Book a free demo at  
[www.acamsriskassessment.com](http://www.acamsriskassessment.com)





# Financial abuse typologies

**T**he Financial Crimes Enforcement Network (FinCEN) has released several publications asking financial institutions (FIs) to be on the lookout for elder financial abuse and to report this abuse when it is identified. While focusing on the elderly, it is a critical function to protect a vulnerable population and this includes legal reporting obligations, where the concept of monitoring for financial abuse can and should be expanded beyond the elderly.

## What is financial abuse?

Financial abuse, also referred to as economic abuse, is defined by the U.S. Department of Justice (DOJ) as follows:

“Controlling or restraining a person’s ability to acquire, use, or maintain economic resources to which they are entitled. This includes using coercion, fraud, or manipulation to restrict a person’s access to money, assets, credit, or financial information; unfairly using a person’s personal economic resources, including money, assets and credit, or exerting undue influence over a person’s financial and economic behavior or decisions, including forcing default on joint or other financial obligations, exploiting powers of attorney, guardianship, or conservatorship, or failing or neglecting to act in the best interests of a person to whom one has a fiduciary duty.”<sup>1</sup>

Financial abuse can affect anyone at any time. Three types of financial abuse include:

- Elder financial abuse
- Domestic financial abuse
- Childhood financial abuse

## Elder financial abuse

The Consumer Financial Protection Bureau (CFPB) reported in September 2022 that a large number of older adults lose money due to elder financial abuse and these victims rarely recover.<sup>2</sup> The DOJ reported that the National Adult Mistreatment Reporting System documented 46,279 victims of adult mistreatment over the age of 60 across 36 states in 2021, with 19,087 or 41% of victims suffering exploitation.<sup>3</sup> In most cases, the relationship to the perpetrator was a family member. The Internet Crime Complaint

Center reports that over 82,000 victims over the age of 60 reported elder fraud, with losses totaling \$3.1 billion in 2022, which is an 84% increase in losses over 2021.<sup>4</sup>

The forms of elder abuse can range from stranger fraud to family exploitation, along with everything in between. Most people are familiar with the concept of romance and grandparent scams, where criminals rely on relationships to obtain funds. But the increasing trend of pig butchering scams, may present a heightened emerging threat to this already vulnerable population. What starts as a seemingly innocent email or phone contact turns into a full-blown scheme to invest in fake offerings, often involving cryptocurrency.<sup>5</sup> Targeting an already lonely and isolated population that tends to be focused on ensuring and solidifying their financial future, pig butchering exploits two basic needs: Human connection and financial security.

Beyond pig butchering, cryptocurrency scams are on the rise according to the Federal Bureau of Investigation's (FBI) 2022 Elder Fraud Report, accounting for over \$1 billion and approximately 66% in losses in 2022.<sup>6</sup> As cryptocurrency becomes a favored source of payment for fraudsters, it is showing up in more conventional fraud typologies, including investment and tech support scams, confidence and romance schemes, and lottery or inheritance ruses. Despite the increase in cryptocurrency fraud, consumers over 60 remain underrepresented in the cryptocurrency market. While they represent nearly 32% of the U.S. adult population, they only represent 10% of cryptocurrency owners.<sup>7</sup> Fraudsters are reaping significant benefits from feeding on the need for financial security among a population conventionally seen as naïve about technology and new investment strategies.

Another emerging scam, an adaptation of well-known tech support schemes, is referred to as the "phantom hacker" scam. The FBI issued an alert on September 29, 2023, warning the public to be vigilant regarding this new twist on an existing scam. This multistep scheme involves two to three individuals advising a victim that their accounts are compromised and that they need to move their money to a "safer" third-party location.<sup>8</sup> In the first half of this year, the FBI reported 19,000 victims with losses of more than \$542 million, noting that almost 50% of the victims were over 60 years old.

Further, gaps remain in the process of recovering funds for victims of elder financial abuse. The CFPB reports that key impediments to the identification of elder financial abuse and recovery include the victim having a relationship with the perpetrator, cognitive decline, subpar responder training and resources, and the method and dollar amount of transactions (for instance, fraud involving large dollar

## Lack of access to funds or assets is often a barrier to leaving an abusive situation as there is no way to pay for hotels, apartments, food or other necessities

amounts and transactions via credit or debit cards are easier to detect), among other challenges.<sup>9</sup> Throughout the report, the CFPB identifies ways FIs should be helping:

- Identifying elder financial abuse based on changes in a customer's banking patterns or behavior toward a caregiver
- Contacting customers when there are unusual debit or credit card purchases
- Training staff to identify the signs of elder financial abuse
- Investigating activity when reported by the customer
- Understanding reporting responsibilities beyond Bank Secrecy Act obligations, such as state-mandated reporting

### Domestic financial abuse

The National Network to End Domestic Violence (NNEDV) reports that financial abuse occurs in 99% of domestic violence cases and is often cited by survivors as the primary reason survivors stay or return to an abusive partner.<sup>10</sup> Domestic abuse is an epidemic across the world with more than 10 million women and men suffering physical abuse by an intimate partner annually.<sup>11</sup> The National Coalition Against Domestic Violence reports that the cost of domestic violence exceeds \$8.3 billion per year with survivors losing eight million days of work and 21%-60% losing their jobs for reasons related to the abuse.<sup>12</sup> But there is something FIs can do to help. The red flags associated with financial abuse are similar to red flags monitored today for elder financial abuse and human trafficking (HT).



The NNEDV notes that financial abuse is one of the most powerful ways abusers keep survivors in the abusive relationship.<sup>13</sup> Lack of access to funds or assets is often a barrier to leaving an abusive situation as there is no way to pay for hotels, apartments, food or other necessities. Survivors report, on average, having access to less than \$290 while needing an average of nearly \$800 a month to stay independent and safe.<sup>14</sup> Defaulting on joint credit and coerced debt ensures survivors may not qualify for a variety of credit-based services such as housing rentals, auto loans or utility services.

Similar to HT cases, abusers may retain possession of the survivor's identification documentation. That, coupled with restricting access to financial information and funds, can impede a survivor's access to the banking system. That access may be critical to a survivor leaving their situation.

### Childhood financial abuse

In 2021, the U.S. Department of Health and Human Services reported that 588,229 children would become victims of child abuse and neglect, based on nearly four million referrals of child maltreatment to child protective services across the U.S.<sup>15</sup> Reports are broken into physical, sexual and psychological abuse, as well as neglect, meaning information on financial abuse is not separately tracked. A form of psychological abuse, childhood financial abuse is defined as the act of using money as a weapon to take advantage of a minor, typically taking one of three forms: Parental financial abuse, identity theft and teen financial abuse.<sup>16</sup>

Parental financial abuse and teen financial abuse mimic many of the same behaviors and red flags as domestic financial abuse and elder financial abuse. However, given the guardian/child relationship, the activity may be more difficult to detect. The most prevalent and unidentified is when a parent or guardian uses a child's information to obtain a loan or purchase items they cannot afford. According to Syracuse University, the impacts often go undetected until after significant damage is done.<sup>17</sup> This form of identity theft is detrimental to minors coming of age who may not be able to obtain credit on their own due to poor credit history.




Identity theft is a rising concern for children. According to the National Foundation to End Child Abuse and Neglect, children are 50 times more at risk of being victims of identity theft than adults due to their lack of credit history coupled with the fact that children do not have a need to check their credit scores.<sup>16</sup> This results in a keen opportunity for thieves to use a relatively clean slate and go undetected.

### How can FIs help?

There are three primary ways FIs can help:

1. Monitor for red flags that might indicate all forms of financial abuse and emerging scams and issues.
2. Train employees and customers to monitor for red flags and share bulletins on emerging schemes and issues as they are made available.
3. Design programs to assist with opening accounts for vulnerable populations regardless of age.

### Conclusion

Financial abuse is a broad problem that can impact all populations in a variety of ways, and FIs are in a keen position to provide a safer banking environment for survivors, identify additional criminal activity and possibly save more lives. This is another way to accomplish the goal of providing a banking system that is safe and accessible to everyone while rooting out criminal activity that puts customers at risk. 

Stephanie Bye, CAMS,  
SVP Financial Crimes, WA, USA,  
sbye@quonticbank.com

- <sup>1</sup> "Domestic Violence," *Office on Violence Against Women, U.S. Department of Justice*, <https://www.justice.gov/ovw/domestic-violence>
- <sup>2</sup> "Recovering from Elder Financial Exploitation," *Consumer Financial Protection Bureau*, September 2022, [https://files.consumerfinance.gov/f/documents/cfpb\\_recovering-from-elder-financial-exploitation\\_report\\_09-2022.pdf](https://files.consumerfinance.gov/f/documents/cfpb_recovering-from-elder-financial-exploitation_report_09-2022.pdf)
- <sup>3</sup> "EAPPA Data Overview," *U.S. Department of Justice*, <https://www.justice.gov/elderjustice/eappa>
- <sup>4</sup> "Elder Fraud," *Internet Crime Complaint Center*, [https://www.ic3.gov/Content/PDF/Elder\\_Fraud\\_Tri-fold.pdf](https://www.ic3.gov/Content/PDF/Elder_Fraud_Tri-fold.pdf)
- <sup>5</sup> "Pig Butchering" Scams: What They Are and How to Avoid Them," *FINRA*, December 13, 2022, <https://www.finra.org/investors/insights/pig-butcherer-scams>
- <sup>6</sup> "2022 Elder Fraud report," *Federal Bureau Investigation*, [https://www.ic3.gov/Media/PDF/AnnualReport/2022\\_IC3ElderFraudReport.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf)
- <sup>7</sup> James Royal, "Cryptocurrency statistics 2023: Investing in Crypto," *Bankrate*, August 31, 2023, <https://www.bankrate.com/investing/cryptocurrency-statistics/>
- <sup>8</sup> "Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings," *Federal Bureau of Investigation*, September 29, 2023, <https://www.ic3.gov/Media/Y2023/PSA230929>
- <sup>9</sup> "Recovering from Elder Financial Exploitation," *Consumer Financial Protection Bureau*, September 2022, [https://files.consumerfinance.gov/f/documents/cfpb\\_recovering-from-elder-financial-exploitation\\_report\\_09-2022.pdf](https://files.consumerfinance.gov/f/documents/cfpb_recovering-from-elder-financial-exploitation_report_09-2022.pdf)
- <sup>10</sup> "About Financial Abuse," *The National Network to End Domestic Violence*, <https://nnedv.org/content/about-financial-abuse/>
- <sup>11</sup> "National Statistics," *The National Coalition Against Domestic Violence*, <https://ncadv.org/STATISTICS>
- <sup>12</sup> Ibid.
- <sup>13</sup> "About Financial Abuse," *The National Network to End Domestic Violence*, <https://nnedv.org/content/about-financial-abuse/>
- <sup>14</sup> "Before and Beyond Crisis: What Each of Us Can Do to Create a Long-Term Ecosystem of Support for All Survivors," *FreeFrom*, p. 34, <https://www.freefrom.org/wp-content/uploads/2022/08/Beyond-Crisis-PDF.pdf>
- <sup>15</sup> "Child Maltreatment 2021," *U.S. Department of Health & Human Services*, 2023, <https://www.acf.hhs.gov/cb/data-research/child-maltreatment>
- <sup>16</sup> "What is Financial Child Abuse?" *The National Foundation to End Child Abuse and Neglect*, <https://endcan.org/2021/10/21/3-forms-of-financial-child-abuse/>
- <sup>17</sup> "Financial Abuse in a Child/Parent Relationship," *Syracuse University*, October 17, 2022, <https://financialaid.syr.edu/financialliteracy/2022/10/17/october-2022-financial-abuse-in-a-child-parent-relationship/>
- <sup>18</sup> "What is Financial Child Abuse?" *The National Foundation to End Child Abuse and Neglect*, <https://endcan.org/2021/10/21/3-forms-of-financial-child-abuse/>

## AML Foundations for Private Banking and Wealth Management

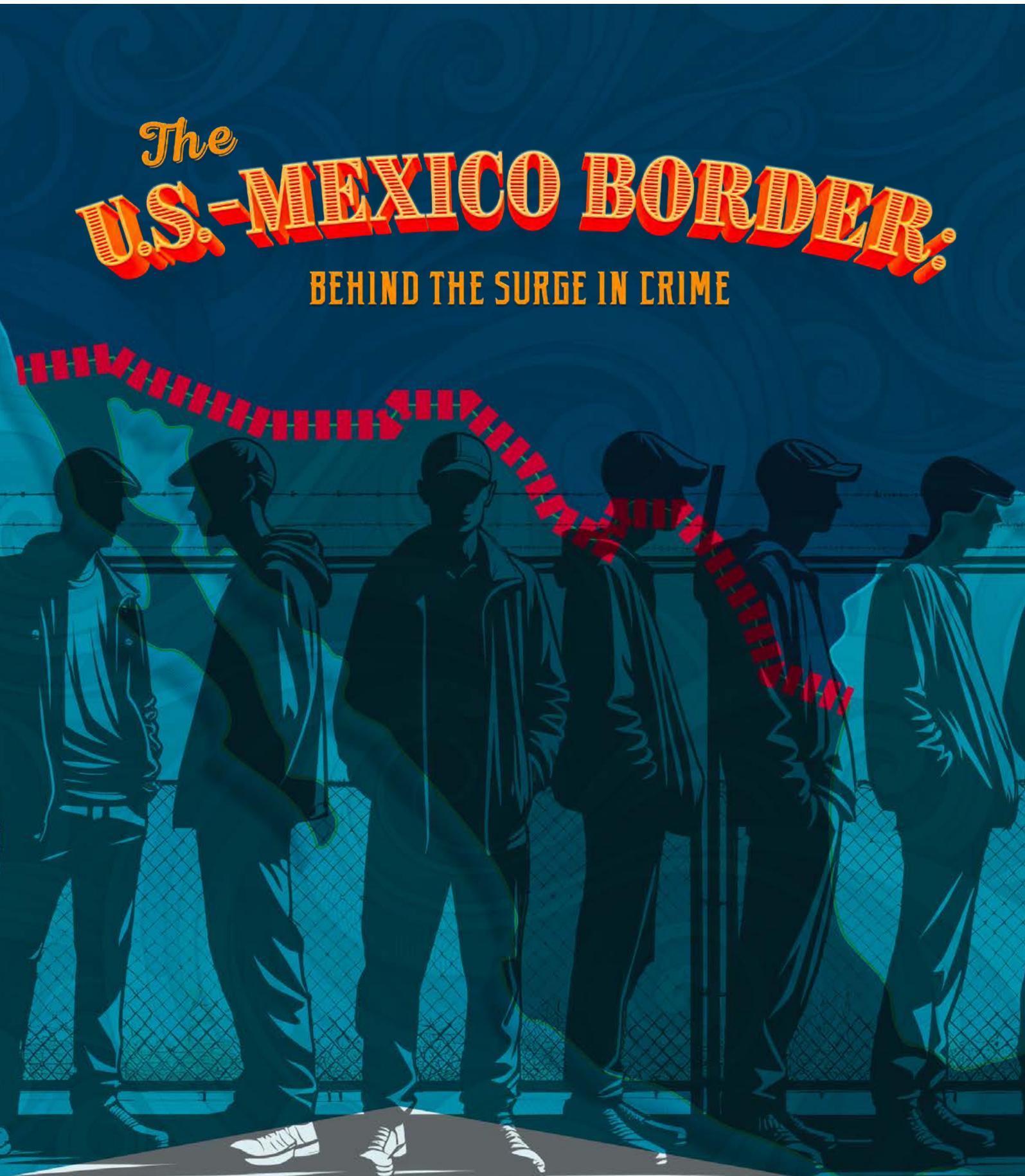
Learn the fundamentals of anti-money laundering in the context of private banking and wealth management with this **new** certificate course.

- Online and self-paced
- Four hours of coursework
- 20-question assessment
- Earn four ACAMS credits

Register now:

[acams.org/en/amlf-pbwm](https://acams.org/en/amlf-pbwm)





The southwestern border of the U.S., spanning 1,954 miles, is more than a geopolitical boundary between the U.S. and Mexico. Its vast expanse has become synonymous with both opportunity and challenges over the years. While many think of trade, commerce and cultural exchange when considering this region, ignoring the undertow of illicit activities is impossible—the border remains a hot spot for drug trafficking, illegal arms trade, human trafficking (HT) and smuggling operations, necessitating vigilant scrutiny and transaction monitoring within the U.S. financial system.

Financial institutions (FIs) are tasked with understanding the concerns along the U.S.-Mexico border and incorporating these considerations into their Bank Secrecy Act (BSA) policy and procedures. It is critical to monitor for suspicious activity to ensure proceeds from these illicit activities do not infiltrate the U.S. financial system, and regulators will expect it.

### Significant threats on the border

**Drug trafficking:** The border is a primary entry point for illicit drugs coming into the U.S. from Mexican drug cartels. The Sinaloa Cartel and the Jalisco New Generation Cartel (CJNG) have extensive networks that smuggle narcotics into the U.S., including marijuana, methamphetamine, cocaine, heroin and fentanyl. Such drug operations require significant sums of money to maintain. Money transfers, cash activity and other financial indicators can lead to funding sources and financial beneficiaries, making it essential for institutions to be on high alert. In 2019, the Financial Crimes

Enforcement Network (FinCEN) issued an “Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids”<sup>1</sup> to alert FIs of illicit schemes related to the trafficking of these deadly drugs. The advisory describes several typologies and red flags to assist in suspicious activity monitoring.

Fentanyl crossing the border is a crisis that must be considered when developing an anti-money laundering (AML) program. According to the National Institute on Drug Abuse (NIDA), deaths involving synthetic opioids, primarily fentanyl, continued to rise, with 70,601 overdose deaths reported in 2021.<sup>2</sup> In 2022, NIDA reported that 109,680 people died as the fentanyl crisis deepened.<sup>3</sup> According to a 2019 FinCEN advisory, the U.S. is in “an unparalleled epidemic of addiction and death fueled by the illicit trafficking, sale, distribution, and misuse of fentanyl and other synthetic opioids.”<sup>4</sup> Transnational criminal organizations (TCOs), “international drug traffickers, money launderers and other criminal actors profit off the misery of victims. Criminal networks and others generate billions of dollars in illicit drug proceeds and use the U.S. financial system and economy to advance their criminal enterprises and continue this epidemic to generate more criminal profits, resulting in more deaths and addictions.”<sup>5</sup> FIs should monitor transactions to and from China, in particular, as the sale or purchase of fentanyl often involves money transfers to individuals in China and other foreign countries. The transactions are usually structured to evade BSA reporting.

**HT and smuggling:** Apart from regular migration, there are instances of people being trafficked or smuggled across the border for forced labor, sexual exploitation or criminal activities. Human smuggling is defined by the United Nations<sup>6</sup> as “the facilitation, for financial or other material gains, of irregular entry into a country where the migrant is not a national or resident. The criminals behind this highly profitable business seize the opportunity created by the need or desire of people to escape not just poverty and lack of employment opportunities but also natural disaster, conflict or persecution.”<sup>7</sup> While smugglers, or “coyotes,” prey on these vulnerabilities, many migrants die of thirst in deserts, perish at sea or suffocate in containers in a desperate search for a better life.

As mentioned by the Rural Health Information Hub, “The Department of Homeland Security defines human trafficking as using force, fraud, or coercion in exchange for labor, services, or a commercial sex act.”<sup>8</sup> The illegal trafficking of humans is a multi-million-dollar industry. Tracking payments, especially large or recurring ones, to familiar sources in border regions could signify involvement in such activities.

While a separate crime, HT gets a lot of exposure in the media and attention from law enforcement (LE). However, its sister crime—human smuggling—can be just as deadly. Human smuggling is not a victimless crime, as evidenced by the San Antonio, Texas, discovery in June 2022 of 53 migrants, including children, who died in a tractor-trailer as they attempted to enter the U.S. illegally.<sup>9</sup> The smuggler abandoned the locked trailer in sweltering South Texas temperatures with no water, and the people perished. This example is only one of the many yearly tragedies along our southwest border.

HT and smuggling have been named as part of FinCEN’s National Priorities, and FIs should include these concerns in their risk assessment and AML program. In January 2023, FinCEN issued an alert on human smuggling along the U.S.

southwest border, FIN-2023-Alert001.<sup>10</sup> The alert emphasizes the seriousness of the crime, which can endanger lives because criminal organizations value profits over human souls. The southwest border is a hotbed for this crime, where over 2.3 million encounters occurred in 2022, up from 1.7 million in 2021 and growing.<sup>11</sup> According to the Homeland Security Operational Analysis Center, criminals on the southwest border conducting human smuggling generate an estimated revenue of \$2 billion to \$6 billion annually.<sup>12</sup>

FIs can detect and report human smuggling if red flags are identified. In addition to the two FinCEN advisories released in 2014<sup>13</sup> and 2020,<sup>14</sup> the 2023 alert gives several red flags specific to threats along the southwest border, such as frequent cross-border wire transfers, rapid movement of funds and deposits followed by immediate withdrawals (funnel accounts).

**Illegal arms trade:** The U.S. has long been a source of military-grade firearms smuggled into Mexico that end up in drug cartels' hands. As reported by CBS News,<sup>15</sup> this illegal arms trade has fueled violence in Mexico, which has spilled into the U.S. border cities at an alarming rate. Cartel gunrunning networks operate like terrorist cells and pay Americans to buy weapons from gun stores and online dealers nationwide.


In a press release,<sup>16</sup> the U.S. Department of the Treasury announced the sanctioning of a well-known Mexican arms trafficker in September 2023 for supporting the CJNG, among other violations. "CJNG relies on high-powered weapons primarily obtained from the U.S. to protect its territory while intimidating rivals and governmental authorities," said Under Secretary of the Department of the Treasury Brian E. Nelson.<sup>17</sup> "CJNG's access to these weapons contributes to its

## Fls can detect and report human smuggling if red flags are identified

ability to flood the United States with fentanyl and other deadly drugs. Treasury is working with U.S. and Mexican partners to expose, isolate, and disrupt those who facilitate CJNG's lethal activities."<sup>18</sup> The Department of the Treasury's action is part of a government effort to stop arms and drug trafficking across the U.S. southwest border.

**Potential terrorist entry:** One of the most pressing threats to the U.S. is the movement of potential terrorists or extremist elements. Intelligence agencies have raised alarms about extremist individuals exploiting the vastness of this border to enter the U.S. The confluence of these terrorism threats underscores the critical importance of a comprehensive approach to monitoring activity at the southwest border. While the numbers are debated and may be low compared to other threats, there is concern about the potential for extremist individuals or groups to exploit vulnerabilities at the border to enter the U.S.<sup>19</sup> According to NBC News, this year, U.S. border agents have encountered a "growing number of individuals"<sup>20</sup> on the Federal Bureau of Investigation's terrorist watchlist, including U.S. citizens,<sup>21</sup> stopped at the southern border. The most significant threat of terrorist activity is from immigrants from the Eastern Hemisphere, including Africa and the Middle East, which has more than doubled in 2023 to 228,000 from 110,000 in 2022.<sup>22</sup>

### Conclusion

The U.S.-Mexico border is a focal point of numerous illicit activities that require vigilant oversight by LE and Fls. Recognizing the signs of illicit financial activity and acting on them is crucial in combating the broader issues plaguing the border. Fls, equipped with FinCEN guidance and a deeper understanding of border-related risks, can become formidable partners in the fight against border-related financial crimes. If there is a hint of suspicion, Fls should dive deeper. In our world of financial crime detection, suspicion might be the thread that unravels a more significant, darker scenario. Fls should tailor their oversight based on varying risk profiles. In the AML arena, knowledge is power. Reporting suspicious activities via suspicious activity reports ensures institutions remain ahead of the curve. 

**Terri Luttrell, CAMS-Audit, board member, ACAMS Central Texas Chapter, compliance and engagement director, Abrigo, [Terri.luttrell@abrigo.com](mailto:Terri.luttrell@abrigo.com), **

<sup>1</sup> "FIN-2019-A006: Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids," *Financial Crimes Enforcement Network*, August 21, 2019, <https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf>

<sup>2</sup> "Drug Overdose Death Rates," *National Institute on Drug Abuse*, June 30, 2023, <https://nida.nih.gov/research-topics/trends-statistics/overdose-death-rates>

<sup>3</sup> Ibid.

<sup>4</sup> "FIN-2019-A006: Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids," *Financial Crimes Enforcement Network*, August 21, 2019, <https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf>

<sup>5</sup> Ibid.

<sup>6</sup> United Nations Office on Drug and Crime homepage, <https://www.unodc.org/>

<sup>7</sup> "Migrant Smuggling," *United Nations Office on Drugs and Crime*, <https://www.unodc.org/unodc/en/human-trafficking/migrant-smuggling/migrant-smuggling.html>

<sup>8</sup> "Violence and Abuse in Rural America," *Rural Health Information Hub*, <https://www.ruralhealthinfo.org/topics/violence-and-abuse>

<sup>9</sup> Ray Sanchez, Nicole Chavez and Priscilla Alvarez, "On a Texas road called 'the mouth of the wolf,' a semitruck packed with migrants was abandoned in the sweltering heat," *CNN*, June 29, 2022, <https://www.cnn.com/2022/06/29/us/san-antonio-migrant-truck-deaths/index.html>

<sup>10</sup> "FIN-2023-Alert001: FinCEN Alert on Human Smuggling along the Southwest Border of the United States," *Financial Crimes Enforcement Network*, January 13, 2023, [https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Human%20Smuggling%20FINAL\\_508.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Human%20Smuggling%20FINAL_508.pdf)

<sup>11</sup> Ibid.

<sup>12</sup> "FinCEN Issues Alert on Human Smuggling Along the Southwest Border of the United States," *Financial Crimes Enforcement Network*, January 13, 2023, <https://www.fincen.gov/news/news-releases/fincen-issues-alert-human-smuggling-along-southwest-border-united-states>

<sup>13</sup> "FIN-2014-A008: Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking - Financial Red Flags," *Financial Crimes Enforcement Network*, September 11, 2014, <https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A008.pdf>

<sup>14</sup> "FIN-2020-A008: Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," *Financial Crimes Enforcement Network*, October 15, 2020, [https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory Human Trafficking 508 FINAL\\_0.pdf](https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf)

<sup>15</sup> E.D. Cauchi, "Mexican drug cartels pay Americans to smuggle weapons across the border, intelligence documents show," *CBS News*, September 18, 2023, <https://www.cbsnews.com/news/mexican-drug-cartels-american-weapons-smuggled-across-border/>

<sup>16</sup> "Treasury Sanctions Mexican Arms Trafficker Supplying U.S.-Sourced Weapons to CJNG," *U.S. Department of the Treasury*, February 28, 2023, <https://home.treasury.gov/news/press-releases/jy1310>

<sup>17</sup> Ibid.

<sup>18</sup> Ibid.

<sup>19</sup> Camilo Montoya-Galvez, "Are terrorists trying to enter the U.S. through the southern border? Here are the facts," *CBS News*, October 11, 2023, <https://www.cbsnews.com/news/us-mexico-border-terrorists/>

<sup>20</sup> Julia Ainsley, "Number of people on terrorist watchlist stopped at southern U.S. border has risen," *NBC News*, September 14, 2023, <https://www.nbcnews.com/politics/national-security/number-people-terror-watchlist-stopped-mexico-us-border-risen-rcna105095>

<sup>21</sup> Julia Ainsley, "CBP stopped two men on terrorism watchlist at border, says such incidents are rare," *NBC News*, April 6, 2021, <https://www.nbcnews.com/politics/immigration/cbp-stopped-two-men-terror-watchlist-border-says-such-incidents-rare-n1263167>

<sup>22</sup> Julia Ainsley, "Number of people on terrorist watchlist stopped at southern U.S. border has risen," *NBC News*, September 14, 2023, <https://www.nbcnews.com/politics/national-security/number-people-terror-watchlist-stopped-mexico-us-border-risen-rcna105095>

# THE ISO 20022 PAYMENT STANDARD: A PARADIGM SHIFT

*Editor's note: Survey distribution, analysis and results were compiled by the author. The views and results expressed are solely those of the author and are not meant to represent the opinions of ACAMS.*

The cross-border payments market was estimated to be worth \$150 trillion in 2017 and is slated to increase to \$250 trillion by 2027.<sup>1</sup> These cross-border payments constitute wholesale cross-border payment transactions as well as retail cross-border payments. As per a recent report, 81% of cross-border payment transactions involved remittances (i.e., money being sent to support friends and families abroad).<sup>2</sup> With this size and with global economies becoming increasingly connected, it is important to have a fast, secure and efficient cross-border payment system.

Various cross-border payment systems are used across the globe, which ensures that financial institutions (FIs) worldwide exchange cross-border-related information securely along with the electronic messages related to these cross-border transactions. Clearing House Interbank Payments System (CHIPS), Fedwire, Single Euro Payments Area (SEPA), Cross-Border Interbank Payment System (CIPS) and Society for Worldwide Interbank Financial Telecommunication (SWIFT) are some of the major cross-border payments systems used globally. SWIFT is the most prominent among these systems, which handles 48% by volume and 56% by value of all cross-border payments.<sup>3</sup>

AS PER A RECENT REPORT,  
81% OF CROSS-BORDER  
PAYMENT TRANSACTIONS  
INVOLVED REMITTANCES

## SWIFT text messaging standards

SWIFT, being a synonym for cross-border payment transactions, started its journey in the 1970s by replacing Telex technology. It revolutionized how different parties of the financial services industry connected and exchanged payment-related information for the execution and settlement of cross-border financial transactions. However, with the increased integration of the global financial system, real-time payments started becoming a reality. Payment systems like SWIFT also started facing challenges, and gradually, the messaging system became more ineffective for global institutions due to its high cost, slow speed and lack of transparency in electronic messages. There were also issues due to fragmented messaging standards, which resulted in data truncation and incorrect processing of payment transactions.

This fragmentation resulted in the absence of complete transaction information in the messaging formats, adversely impacting the identification of financial crime risk (i.e., impeding the sanctions screening process, making it difficult to investigate sanctions alerts and matches). This ultimately resulted in greater exposure to sanctions risk for the FIs.

## The ISO 20022 payment standard

To address the above limitations, the industry decided to replace the existing text messaging standard with the new payment standard, also known as ISO 20022 or the MX messaging format standard. This new standard is based on the extensible markup language (XML) rule. The new payment standard will be a paradigm shift in the cross-border payment industry and will trigger the new progressive world order by further standardizing the messaging formats and ensuring a more cohesive and seamless global trade environment.

The new ISO 20022 payment standard is expected to bring in greater transparency and increased efficiency in the messaging formats, which will ensure the coverage of all the relevant financial transaction information and ultimately reduce operational frictions, facilitate faster payment execution, lower cost and enhance the detection and mitigation of sanctions/financial crime compliance risks.

**THE GLOBAL ADOPTION OF THE NEW ISO 20022 PAYMENT STANDARD IS A MUCH-AWAITED DEVELOPMENT IN THE HISTORY OF CROSS-BORDER PAYMENTS**

**ISO 20022: Benefits and challenges**

The global adoption of the new ISO 20022 payment standard is a much-awaited development in the history of cross-border payments. The changes it will bring to payment messaging formats will have a transformative impact on the financial services industry. However, if one digs deeper into the technicalities, the changes seem to be complicated not only for compliance professionals but also for the professionals working in technology. That is why FIs are following an extremely cautious approach to embedding the new standard into their compliance ecosystem. FIs are approaching the 2025 deadline at different paces, and nearly 70 countries are already using ISO 20022, including Switzerland, China, India and Japan. On the other hand, the transition in Europe is still in the work-in-progress stage, and they are working on adopting the new standard in a carefully crafted strategy. Australia, however, is going hand-in-hand with both payment systems (i.e., text message and MX messaging formats and targeting to fully go live by 2024).

While we discuss the pace of adoption globally, it is important to understand the reason behind this fragmented pace of adoption at a global level. Although there is no doubt about the vast and far-reaching benefits of the ISO 20022 payment standard, some major challenges are impacting the pace at which this standard is getting embedded into the existing system by FIs.

To understand the challenges in the implementation of the ISO 20022 standard, a survey across India and the Asia-Pacific and Middle East regions<sup>4</sup> sought the views from compliance professionals on the benefits and challenges of the new standard.

Out of the total responses received, 93% of the respondents agreed and acknowledged that the new payment standard would be more effective. In terms of their understanding, 67% of respondents perceive that the ISO 20022 standard is the “common messaging standard,” where 22% acknowledged it to be freely implementable and scalable and 11% responded that it is an independent standard. On further advantages, 71% of the compliance/sanction officers acknowledged that the biggest advantage of the new standard would be addressing financial crime compliance risk and improving structured data. Fourteen percent of respondents mentioned the advantage of having a consistent data model, while another 14% acknowledged benefits regarding regulatory reporting.

When they were further questioned on the impact of adopting the ISO 20022 payment standard on the effectiveness of sanctions screening and false positive alerts, 51% of the respondents expected that the false positive alerts would be reduced by more than 30%. Twenty-five percent of respondents expected a reduction in the range of 10% to 30% and 25% expected a reduction below 10%. This optimism regarding the benefits of the name screening process is encouraging and demonstrates confidence in the ISO 20022 standard by the compliance and sanctions officers.

Amid this encouraging response on the benefits, when the question was asked as to what challenges they see for adoption of the ISO 20022 payment standard, 50% of the respondents acknowledged the implementation challenges with respect to their existing compliance systems and 50% responded that understanding the new syntax of the ISO 20022 standard will be the biggest challenge in the adoption.

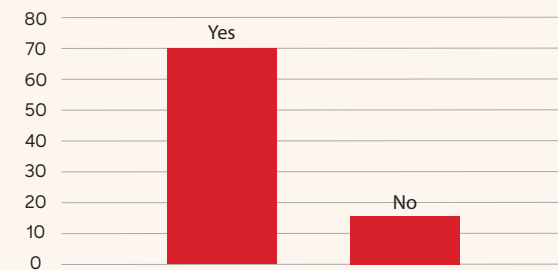
The benefits of this ISO 20022 standard to FIs will include higher data quality, holistic payment transaction information and an enhanced non-fragmented standard messaging format. A snapshot of these key benefits is as follows:

- Enhanced level of data quality and longer character limits
- An effective and efficient sanctions screening process resulting in effective sanctions alert management
- Increased and effective financial crime compliance risk management
- Effective reconciliation of cross-border transactions due to richer data quality
- Enhanced level of interoperability and interface among various payment systems
- Low cost of maintenance and incurring low cost for the execution of faster cross-border payment transactions

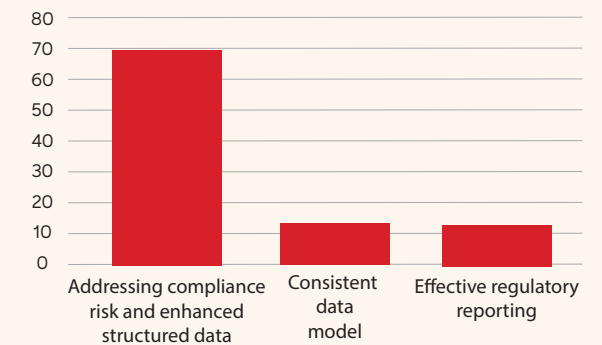
Graphic 1 below is a depiction of the survey respondents' views on the benefits and challenges of the ISO 20022 payment standard.

**Graphic 1: Survey results (in percentages)**

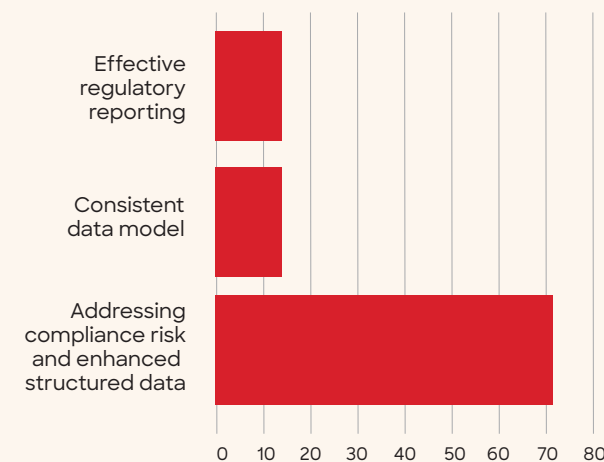
**Will the ISO 20022 standard be more effective in terms of transparency**



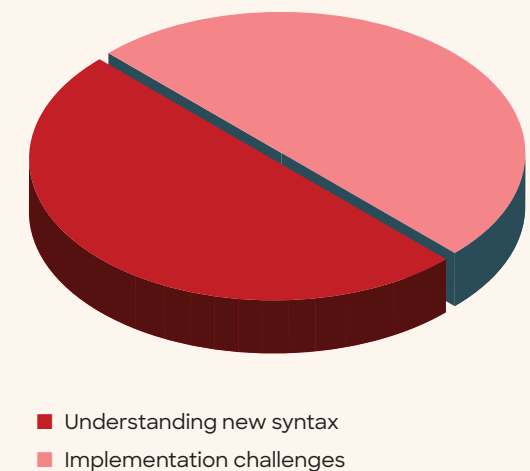
**Advantages of ISO 20022 standard vis-a-vis existing MT standard**



**Benefits of ISO 20022 standard**



**Challenges in the adoption of ISO 20022 standard**



Visualization: Sachin Shah

Source: Survey and results conducted by the author<sup>5</sup>

The above responses obtained from fellow compliance professionals clearly demonstrate that despite the benefits ISO 20022 aims to bring to the table, FIs and compliance officers still must navigate through their “migration” strategy to the new standard. Before one concludes on the required implementation road map, it is worth considering a few more pieces of information obtained during this survey.

The first thing that invites attention is the changes required in the enhancements required in the legacy payment systems. One of the biggest advantages of the new standard is the structured data points, which will bring efficiency to the payment messages by making the message format more standardized and homogeneous. As per the SWIFT publication, “ISO 20022 for Dummies,” the new payment standard has a methodology that can describe business processes and a common business language. It also has the functionality to be rendered in different syntaxes, enabling implementations for messaging and application programming interfaces. Consequently, the ISO 20022 standard is going to address the pain points related to the syntaxes and the semantics and result in a consistent message standard. To embed these functionalities into their existing system is going to be an uphill task for FIs as that will require enhancement to the existing technical specifications of the legacy systems. That will also involve creating the capability to accommodate 775 business components and more than 800 message definitions.<sup>6</sup> In short, the whole technological architecture of the legacy systems will need to be reviewed and enhanced.


The second point is understanding the proposed messaging format of the ISO 20022 payment standard and the related nuances. During


the interaction with fellow compliance/sanction professionals, one of the compliance officers shared that there are challenges in understanding the new proposed format and a dearth of techno-functional experts who can guide the transition and conversion of the text message format to the new MX message template format at the user analysis and testing phase as well as the production stage of the implementation. To increase the complexity, there is also a shortage of vendors who can support FIs in the transition to the new payment standard. This demonstrates the critical gap in getting support for the transition for FIs.

To summarize the on-the-ground reality, the ISO 20022 payment system is not only the most awaited development in the payment industry but is also going to be the testing time for compliance/sanction officers and FIs globally. However, it is also going to be a “once-in-decade” kind of opportunity where compliance officers will leverage their complete knowledge and wisdom in making this transformational journey a success not only for their respective institutions but also for the industry at a macro level.

### Conclusion

The ISO 20022 payment standard is a much-awaited transformative development in the payment processing industry, which will bring the “element of order” to the whole payment processing ecosystem. The paradigm shift will make payment processing more efficient, faster and transparent. However, banks and FIs need to strategize their transition to the new standard in a very cautious and mature way, keeping in mind the maturity level of their

institution’s payments processing ecosystem and the benefits and challenges discussed above. While FIs gear up to embrace the benefits of the new standard, they also need to overhaul compliance processes and supporting technology. Once the necessary investments in terms of financial budgets, the experience of the subject-matter experts and the thorough overhaul of the entire ecosystem have been undertaken, the ISO 20022 payment standard will truly create a coherent and more transparent financial services payments processing environment. 

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

*Disclaimer: The content contained herein is for general information purposes only and is neither legal nor business advice. You should consult your own legal and business advisors for advice that applies to your specific situation.*

<sup>1</sup> Victoria Cleland, “Victoria Cleland: Global action to enhance cross-border payments,” *BIS*, April 4, 2023, <https://www.bis.org/review/r230404i.htm>

<sup>2</sup> “Cross-border payments: Market overview,” *PWC*, July 2021, <https://www.pwc.in/industries/financial-services/fintech/dp/the-evolving-landscape-of-cross-border-payments.html>

<sup>3</sup> “SWIFT gpi data indicate drivers of fast cross-border payments,” *BIS*, February 8, 2022, [https://www.bis.org/cpmi/publ/swift\\_gpi.pdf](https://www.bis.org/cpmi/publ/swift_gpi.pdf)

<sup>4</sup> The author conducted an independent survey with compliance professionals across India and the Asia-Pacific and Middle East regions.

<sup>5</sup> This survey and its results were created by the author.

<sup>6</sup> “Swift ISO 20022 for Dummies, 6th Edition,” *For Dummies and John Wiley & Sons, Inc.*, 2022.

ACAMSToday.org

# Ask the AFC GURU



Top AFC crime experts answer your questions on a variety of topics covering:

- Career guidance
- Compliance
- Anti-corruption
- AFC trends
- Sanctions

ACAMS  
TODAY



SCAN ME

Keep an eye on ACAMS Today’s LinkedIn and X pages for the next guru

# AI and the FDIC's disaster-related regulatory adjustment

In September, the Federal Deposit Insurance Corporation (FDIC) decided to ease regulatory restrictions on banks and financial institutions (FIs), particularly in the context of disaster relief, an important and needed practice.<sup>1</sup> Essentially, the FDIC extended the reporting time for risk conditions and the overall health of a financial entity.

This measure is intended to help ensure that FIs can remain in compliance while increasing their focus on addressing immediate concerns for affected customers and workers. As the rules come into effect, much can be done to maximize the effectiveness of this latest regulatory relief. Allowing organizations to reduce regulatory pressure during an unforeseen disaster is always good practice and allows them to prioritize safety and soundness over reporting. That said, not all circumstances are alike.

## In practice

It is important to consider that some potential drawbacks might include delays in extracting financial data from the silos of stored information, making it more difficult for regulators, investors and the public to assess the financial health of affected institutions. With that in mind, it was prudent for the FDIC to strike a balance between providing this flexibility and transparency with regulatory oversight, something attainable under the new regulatory regime.

For example, for consumers who may have used a recently damaged home as collateral for a previous loan, the guidance from the FDIC may grant much-needed breathing room in making payments. It seems fair that, as a family may face temporary homelessness due to natural disasters, the FDIC is encouraging institutions not to make this permanent owing to a change in the value of the asset.

Moreover, during natural disaster events such as hurricanes, floods and wildfires, banks face various challenges in terms of operational continuity. However, banks and FIs might also want to call upon artificial intelligence (AI) to come to the rescue for customer care and risk management during such difficult times.

## Using AI

AI plays a critical role in helping to predict and analyze historical data, weather patterns and other relevant information to forecast natural disasters and minimize financial impacts.

While the implementation of AI can help track and monitor secure digital transactions, it can also detect potentially fraudulent activities that may increase during or after natural disasters. It has an inherent ability to assess portfolio risks, helping banks make more informed decisions about risk management implementation.

In order to get ahead of potential threats and unusual transactions or patterns, AI can also help delegate responsibilities to the workforce. In a crisis, new technologies can be a reinforcement from senior management all the way down to the teller level. AI works in real time and can be integrated with the early alerts and warning signs to identify all these vulnerabilities and take the necessary steps to reallocate infrastructure or relocate critical operations and personnel where needed.

We have all seen the AI-driven chatbots and automated pop-ups where websites wish to help communicate with customers, and they can also provide tangible information to and from the customer's user interface and the local, regional or national bank level. These AI-powered virtual assistants can handle routine customer service inquiries, freeing up personnel to focus on the more complex tasks and actions needed during a time of vulnerability.

While these are attainable add-ons to any business today, on the back end, AI can assist in a barrage of services, including automating data recovery and backups even when physical data centers may seem to be compromised; they can ensure regulatory compliance and can help banks and FIs keep track of reporting requirements and provide necessary assistance in meeting them.



## Conclusion

Thinking about risk assessment and mitigation measures ahead of time is always critical, but in the aftermath of a disaster, AI technologies can be implemented. Online banking solutions that reach more consumers via mobile banking units, temporary branches or even virtual customer support can compensate for the downtime of brick-and-mortar locations and effectively leave the lines of communication open for customers during potential service disruptions, allowing customers to access their accounts and ledgers. Such measures also enhance employee safety as they can be accomplished via remote work.

By encouraging banks to think creatively about the community support that the FDIC is advocating, it is important to note that human expertise is still an essential tool in assessing the context and making critical decisions during a natural disaster. Considering the viability of AI as part of a bank's overall risk management approach, the impact of future natural disasters on financial viability can be minimized. That can only be a good thing. **AI**

**Matthew Leaney**, chief revenue officer, *Silent Eight*, New York, USA, [matthew.leaney@silenteight.com](mailto:matthew.leaney@silenteight.com), [@\\_SilentEight](https://www.instagram.com/_SilentEight), [in](https://www.linkedin.com/company/silenteight)

<sup>1</sup> For an example of a decision made to ease regulatory restrictions to financial institutions in areas affected by disaster, view: "Financial Institution Letter: Regulatory Relief—Guidance to Help Financial Institutions and Facilitate Recovery in Areas of Florida Affected by Hurricane Idalia," *Federal Deposit Insurance Corporation*, September 1, 2023, <https://www.fdic.gov/news/financial-institution-letters/2023/fil23048.html>

## 2023 Lifetime Achievement Awards

**John J. Byrne, Esq., CAMS,**  
executive vice president and chairman,  
Advisory Board, AML RightSource



**J**ohn J. Byrne, Esq., CAMS, is executive vice president and chairman of the Advisory Board at AML RightSource. He is also an adjunct professor at George Mason University's Schar School of Policy and Government.

Byrne is an internationally known regulatory and legislative attorney who has been one of the leading AML community voices for over 35 years. He has experience in a vast array of financial service-related issues, with particular expertise in regulatory oversight, policy and governance, anti-money laundering (AML), privacy and terrorist financing. Byrne, who had previously served as the executive vice president of ACAMS, has written hundreds of articles and blogs on AML, financial crime and privacy; represented the financial sector in this area before the U.S. Congress, state legislatures and international bodies such as the Financial Action Task Force (FATF); and appeared on CNN, *Good Morning America*, *The Today Show* and many other media outlets in the U.S. and abroad.

Byrne has received numerous awards, including the *Director's Medal for Exceptional Service* from the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), the American Bankers Association's (ABA) *Distinguished Service Award* for his work in the compliance field, the Patricia Wise Award from the West Coast AML Forum (WCAML), as well as several awards for writing and for his podcast, "AML Now" (which has

## John J. Byrne: The birth of an industry

become "AML Conversations"). Byrne was recognized with the *ACAMS Lifetime Service Award* in September 2017. He also serves on Marquette University's Commercial Banking Board and a number of other boards and steering committees.

In addition, Byrne is a member of the United States Running Streak Association (USRSA) for running three-plus miles a day for 26 years and counting.

**ACAMS Today (AT):** *Could you tell us when you started in the anti-financial crime (AFC) industry?*

**John J. Byrne (JB):** First, we never called it the AFC industry—that is a recent acronym. I started in the industry in 1985. This was even before we had money laundering laws on the books in the U.S. As a young lawyer for the American Bankers Association, I was given the project of looking at "The Cash Connection," a report of the President's Commission on Organized Crime under President Reagan. The report looked at whether we needed laws and regulations to deal with the movement of what we now call illicit funds. We started to call the field "anti-money laundering" in the mid-'90s, although it encompassed AML, counter-terrorist financing (CTF) and sanctions. The recent generation has embraced the AFC term.

I have been fortunate enough to be on the ground floor of many of the changes throughout three decades. In 1986, the Money Laundering Control

Act was passed, and then the regulations came out in 1987. At the ABA in 1987, we went on road trips to approximately 20 cities to explain to bankers the new laws and regulations required. So, we would jump on a plane and go to Chicago. Then, we would jump on another plane and go to Seattle. Then we would spend the day at a hotel with 300 or 400 people in the audience, telling them what the laws and regulations require of them. So that's how this all started.

**AT:** *With over 35 years of experience in the anti-financial crime (AFC) industry, what do you consider as your biggest professional accomplishment?*

**JB:** Well, I've been fortunate to be involved in several important organizations including the ABA. We worked extremely hard with the membership to collaborate with both the regulators and law enforcement (LE) so that both sides of the issues related to money laundering were supported. We had our share of arguments, but we always worked closely together. That set the stage for the environment that we're in now. While we in the private sector might be potentially critical about a new law or regulation, it comes from wanting to ensure that we get the right things accomplished.

Back in the '80s and '90s, you could offer possible changes to laws and regulations, and if they made sense, members of Congress on both sides of the aisle would accept them.



In terms of legislation, one thing that I'm most proud of is drafting the first proposal for what became the Bank Secrecy Act Advisory Group (BSAAG). In 1990, we wrote that there should be an organization run by the U.S. Department of the Treasury or FinCEN comprised of members of the private and public sectors working together. I am proud to say that the BSAAG still exists today because it's all about partnership.

**AT:** *What is so important about public-private partnerships? Do you think we've progressed? Do you think we've improved public-private partnerships since you started?*

**JB:** When I was at the ABA, we knew public-private partnerships were important. For instance, I would go to a banking school in Norman, Oklahoma, and appear on panels with Internal Revenue Service agents to talk and train the bankers together. Bankers saw the value of the information to LE and the challenges of compliance from our

perspective. The AML community has always been supportive of our colleagues in the public sector. But as I said before, we can be critical of something—either the process or a proposal—but that doesn't mean we don't have the same goals. Everyone knows how important it is to get information into the hands of LE as quickly as possible so they can detect and prosecute. I think we've definitely improved. We started in a good place, but it's even better now because LE wants to be part of the dialogue and discussion, whether it's an ACAMS assembly or another event. During my time at ACAMS, we made sure that at least one of the issues of *ACAMS Today* would be dedicated to our LE partners. That was always important, both as a message and for content.

**AT:** *In your opinion, what regulatory action would be most beneficial for the AFC industry?*

**JB:** We're all aware of the Anti-Money Laundering Act of 2020, which was signed into law in January

2021, and there are a series of provisions that still aren't finalized that would really be both innovative and essential. For example, one is regulator training. Our examiners are trained, but they sometimes get trained in a way that could be argued is antithetical to AML because it focuses more on the process than the mission. It's not necessarily their fault that they may focus more on a late filing or a missed filing versus the institution's ability to detect and report activity but that is an area that needs to be better addressed. Hopefully, some of the new AML provisions will eventually include investment advisors, the real estate industry, those who sell and purchase antiquities and the art market. When I think back to when the USA PATRIOT Act passed, we advocated that anybody with a financial footprint should be covered under the Bank Secrecy Act (BSA). There should be no exceptions. Hopefully, that will happen.

Also, I would like to mention that reporting could be more efficient. As we know, a large portion of data

points in suspicious activity reports (SARs) are structuring transactions, and those are important to LE. Perhaps if banks and others file a quick SAR versus extensive narratives, LE could get this information quickly. So, let's focus on the important areas where you need descriptions and narratives and let's automate some of the other reports. This will usher in more innovation for the industry.

**AT:** *What recommendations would you give to AFC professionals on how to combat financial crime more effectively?*

**JB:** Be curious and pay attention to current events because that often dictates potential laws and regulations and what the regulators or LE believe is important. There are many ways to stay on top of things domestically and internationally. Make sure people internally (where you work), understand what you're doing because everybody has a role. So, if I'm an AML professional, I'm not going to work in a silo; I'm going to explain to the frontline staff why we're doing what we do. Business lines need to understand that strong compliance equals strong business and it's not a negative. Many people in the business line think of compliance as simply a cost center, but it's a cost-saving center. Be curious, pay attention and get out of your silos.

**AT:** *How can FIs best incorporate artificial intelligence (AI) to combat financial crime?*

**JB:** First, you must get smart people to understand the mission. We have AI experts. I'm certainly not one, but I think that you need to understand that while AI can be used in a useful way, it can also be harmful. I would like to see (and I'm sure this is already happening) the government put together a group of experts, both on the LE side and the technology side, who will figure out how to

continue to get good information. A concern that I have heard in the industry is how do we allow institutions to experiment with AI without criticizing them for regulatory problems during that process? I've talked with many bankers who have said that they are happy to change their technology, but while they do it, they want the possibility of not being criticized by regulating agencies if they miss something. To implement new technology, you need to be able to make mistakes. Perhaps some pilot programs are the best way to do this.

**AT:** *Having achieved a successful career, what would you like to accomplish in the next five years?*

**JB:** I've been fortunate to be teaching a class at George Mason University Schar School of Public Policy on money laundering, terrorism and corruption for the past five years. That's eye-opening because graduate students are interested in this space. They produced a great deal of quality content, which we've been able to post on our websites and LinkedIn. I want to continue teaching and encourage the next generation to be involved in the AML industry.

Another career milestone that I will continue with as long as I keep working is the AML Partnership Forum, which we created in the past two years and are doing again in March 2024. We patterned the Forum after the West Coast AML Forum, which has been going strong for 30 years. The Forum gets LE personnel, private sector professionals and regulators together in a closed-door setting. There's no press or exhibit hall and it's designed to be an exchange of information. Attendance is capped at 180-200 participants to guarantee excellent dialogue and exchange of ideas. That's what we've been able to do here in D.C. and I

want to keep doing that for as long as I can. We made it a self-sustaining 501(c)(3) organization. It's run by private sector people, the Department of Homeland Security, the Internal Revenue Services-Criminal Investigation and the Federal Bureau of Investigation, so it is a perfect public-private partnership event.

In addition, I've now done around 500 or 600 podcasts over the past five or six years. I've visited and interviewed investigative journalists, regulators, people in AI, financial technology (fintech), the sanctions space and other experts—and it's all connected to national security and financial crimes. So, I would like to continue interviewing interesting individuals.

**AT:** *What is the most important lesson you learned while working in the AFC industry?*

**JB:** Everybody's committed. It's a three-legged stool: LE, the private sector and the regulators. Nobody is doing things they don't believe in, which is important to know and refreshing. I'm as cynical as the next person, but then you look at what the community has been able to accomplish.

This is now a career path—it didn't used to be—which is excellent. My daughter Rachele is in this space and I couldn't be prouder. I want to see the next generation after her get involved. All in all, what we do matters. What you do matters. Hopefully, what I do matters. The biggest thing I've learned: This isn't a "check-the-box" industry or community. This is an industry that gets things done. **AT**

*Interviewed by: Karla Monterrosa-Yancey, CAMS, editor-in-chief, ACAMS, editor@acams.org, [in](#)*



Pictured left to right are Markus Schulz, John J. Byrne and Mariah Gause.

## 2023 Lifetime Achievement Awards

**Rick Small, CAMS,**  
executive vice president,  
director, Financial Crimes,  
Truist Financial Corp.



## Rick Small: A storied career in AFC

**R**ick Small leads the Financial Crimes team for Truist, which includes managing anti-money laundering (AML) compliance, controls and investigations, fraud management, internal and external investigations and physical security. He joined Truist in 2016 as the first Financial Crimes program director.

With over 35 years of experience in the public and private sectors, Small was the senior advisor for Anti-Money Laundering and Financial Crimes with Ernst & Young; the senior vice president, Enterprise-Wide Anti-Money Laundering, Anti-Corruption and International Regulatory Compliance for American Express; and the global AML leader for GE Money, a division of General Electric. Small began his private sector career as managing director, Global Anti-Money Laundering for Citigroup.

Prior to these private sector roles, he held several positions with the U.S. government, first as a federal prosecutor with the U.S. Department of Justice in the Antitrust Division and then with the Organized Crime Strike Force, followed by his role as senior counsel for law enforcement at the U.S. Department of the Treasury. His most recent government position was on the staff of the Board of Governors of the Federal Reserve System as deputy associate director in the Division of Banking Supervision

and Regulation. Small is a member of the Advisory Board of ACAMS and a past chairman of the board.

**ACAMS Today (AT):** *With over 35 years of experience in the anti-financial crime (AFC) industry, what do you consider your biggest professional accomplishment?*

**Rick Small (RS):** I would be remiss if I didn't say that the biggest accomplishment for me was, and continues to be, meeting all of the fantastic, like-minded folks who are dedicated to the fight against money laundering and view this as a mission and a calling rather than a job.

As to specific accomplishments, the prosecution of Bank of Credit and Commerce International (BCCI), for those who remember, was a significant victory for the government and for me personally. The development of several regulations, including suspicious activity reporting and co-authoring the first Bank Secrecy Act (BSA) examination manual, were also significant milestones for me.

**AT:** *Having served in the public and private sectors, what would you say is the biggest challenge in implementing effective public-private partnerships to deter financial crime?*

**RS:** In the immediate days after 9/11, when I had just left the government for the private sector, I

reached out to my now very good friend Dennis Lormel, who, at the time, was a senior official in the Federal Bureau of Investigation. We were able to quickly coalesce a group from both the public and private sectors to work very closely over a number of months with the common goal of protecting the U.S. from further attacks and tracking down perpetrators. I use this as an example of the public-private partnership working at its best. While partnerships continue today, given all of the priorities, it is sometimes difficult to identify, focus on and commit resources to the most important priority, which can negatively impact some partnerships.

**AT:** *In your opinion, which regulation has been the most valuable to the AFC industry?*

**RS:** Suspicious activity reporting, in my opinion, is the most valuable regulation. At its core, the idea that financial institutions can report suspected illicit activity to the government without recourse to provide the government with the leads it needs to investigate and hopefully prosecute those who are using the financial sector to commit crimes is a fundamental tenant of risk management. Of course, like all regulations, over time, there should be a reevaluation and reassessment as to whether the regulation is still working as intended or if an update or overhaul is required.



Pictured left to right are Markus Schulz, Rick Small and Mariah Gause.

**AT:** As the AFC industry has developed, how has it evolved and what could be done differently to combat financial crime more effectively?

**RS:** We need a sea change move to embrace a risk-based approach that will be fully supported by all aspects of supervisory bodies. The industry has significantly evolved from the early days of the BSA and the USA PATRIOT Act, with the development of increasingly sophisticated technology along with a cadre of subject-matter experts, such as those who are part of ACAMS. With the skillsets of today and the support

of technology, the industry is well positioned to implement and manage a risk-based program that will, in my opinion, provide significant added value to the continued financial crime challenges.

**AT:** Having achieved a successful career, what would you like to accomplish in the next five years?

**RS:** To my previous points, I would love to be a part of a move to a truly risk-based approach. I am also a huge fan of public-private partnerships, so I want to make sure they continue to grow and flourish.

**AT:** What is the most important lesson you learned while working in the AFC industry?

**RS:** Those of us engaged in this fight are all doing so for the exact same reasons—to protect our economy, our customers and our institutions. Unlike other aspects of the business, there is no competition; we are part of one big family! **AT**

*Interviewed by: Karla Monterrosa-Yancey, CAMS, editor-in-chief, ACAMS, editor@acams.org, [in](#)*

ACAMS

## LAW ENFORCEMENT

# Stay Ahead of Financial Crime

ACAMS works with federal, state, and local government officers to help them **stay ahead of criminals** and remain at the top of their game.

Visit our **Law Enforcement Hub** to find essential **anti-financial crime** training and our latest **resources:**

[www.acams.org/lawenforcement](http://www.acams.org/lawenforcement)

## 2023 Lifetime Achievement Awards

**Dan Soto, CAMS,**  
chief compliance officer,  
Ally Financial



## Dan Soto: Leading the charge against financial crime

**D**an Soto was appointed chief compliance officer of Ally Financial in October 2010. In this role, he is responsible for leading the company's compliance efforts in line with applicable laws, rules and company regulatory policies. Soto joined the company as an executive compliance director in September 2009.

Before joining Ally, Soto held several compliance leadership roles within the financial services industry, including positions at Wachovia Bank, Royal Bank of Canada and Bank of America. Soto also served for over 15 years as a bank examiner with the Federal Deposit Insurance Corporation and the Board of Governors of the Federal Reserve System.

Soto has a bachelor's degree in accounting from the University of Nebraska and attended the American Bankers Association's (ABA) Stonier Graduate School of Banking at the University of Delaware. Soto serves on the board of the North Carolina Council on Economic Education, an organization that aims to enhance and advance economic and financial education for K-12 educators and students in North Carolina. Soto also serves on the advisory boards of the ABA's Annual Risk and Compliance Conference, ACAMS and the BSA (Bank Secrecy Act) Coalition, and he serves on the faculty for the ABA's National Compliance School.

**ACAMS Today (AT):** *With decades of experience in the anti-financial crime (AFC) industry, what do you consider your biggest professional accomplishment?*

**Dan Soto (DS):** First, I thank ACAMS and all the opportunities that everyone associated with ACAMS has provided me. On a global basis, ACAMS is the premier leader in providing education and other tools to anti-money laundering (AML) and AFC professionals.

My biggest accomplishment cannot be measured in a single event. What I am most proud of is that I have had a platform to help influence the careers of many compliance and regulatory professionals, and I believe I have done so in a positive manner.

**AT:** *You serve on a board to enhance financial education for K-12 educators and students, what motivated you to focus your expertise in this area?*

**DS:** The board that I serve on allows teachers and students—together with public and private sectors—to pursue knowledge in financial literacy, including through the simulation of investments in stock markets. By starting at such a young age, including in underserved or predominately minority geographies, individuals can overcome poverty and learn to build wealth for themselves and their families.

**AT:** *As a bank examiner, what was the most common mistake or challenge you saw banks facing?*

**DS:** First, I thoroughly enjoyed my time as a bank examiner, both in the field and in the Washington, D.C. headquarters. I'm not sure that there was one common mistake, but the challenges always included—and still do today—balancing the demands of customers, employees and other stakeholders (e.g., investors, regulators). From an AML/financial crimes standpoint, I believe there is no better control than establishing relationships between the public and private sectors to detect and prosecute those who choose to do wrong. Banks that fail to establish routine discussions with regulators and law enforcement (LE) will no doubt miss out on useful information that will help protect their institutions. ACAMS provides these opportunities!

**AT:** *In your opinion, what regulatory action would be most beneficial for the AFC industry?*

**DS:** This is a difficult response because the regulators follow a lengthy and transparent process when promulgating new rules and regulations. However, when it comes to the enforcement of these rules, there are areas of the AFC process that I believe demand more than the citation of violations or supervisory actions. For example, bank AFC professionals spend an inordinate amount of time documenting the reasons they decided against filing a suspicious activity report when an alert has been generated by a technology-driven model. Rather, the focus should be placed on the reports that were filed to determine the usefulness to LE.

**AT:** *Having achieved a successful career, what would you like to accomplish in the next five years?*

**DS:** I still enjoy what I do and have no plans to stop—at least not in the next few years. Once I make that decision, I would still like to be in a position to either serve on a financial institution's board or perhaps instruct at a college or financial literacy nonprofit.

**AT:** *What is the most important lesson you learned while working in the AFC industry?*

**DS:** The most important lesson that I have learned is that what each of us does every single day in the AFC industry is critical in the fight against money laundering, financial crimes and terrorism. I've also learned that each of us cannot do this on our own or even in our own country. AFC is a global issue and has to be fought on a global stage. And this is why ACAMS is so valuable to all of us. I am proud to have been a part of ACAMS from its beginning and just as proud to be given a Lifetime Achievement Award alongside two great friends, Rick Small and John J. Byrne. **AT**

*Interviewed by: Karla Monterrosa-Yancey, CAMS, editor-in-chief, ACAMS, editor@acams.org, [in](#)*

# HONORING THE PROFESSION'S PACESETTERS

This year, four individuals and one ACAMS chapter were recognized with ACAMS Awards for their significant accomplishments within the anti-financial crime (AFC) space. At a special awards ceremony during The Assembly Las Vegas, which was held at the Aria Resort and Casino in November, Chris Bagnall, CAMS-FCI and Sara Crowe, co-authors of the article "Understanding Human Trafficking," were named the recipients of the *ACAMS Today Article of the Year Award*. Toms Platācis, CAMS, the head of Latvia's financial intelligence unit, was announced as the winner of the *ACAMS Rising AFC Professional of the Year Award*. Nicholas Schumann, the U.S. head of Financial Crime Framework, senior vice president at HSBC, was presented with the *ACAMS AFC Professional of the Year Award* for 2023. In addition, the ACAMS Carolinas Chapter received the *ACAMS Chapter of the Year Award* for 2023. Help us celebrate their success by reading more about their achievements in the following interviews with the award winners!

## 2023 ACAMS Today Article of the Year

### Chris Bagnall and Sara Crowe: “Understanding Human Trafficking”

**A**CAMS Today caught up with Chris Bagnall, CAMS-FCI, of Quantexa and Sara Crowe of Citibank, recipients of the 2023 ACAMS Today Article of the Year Award for their co-authored article “Understanding Human Trafficking.”<sup>1</sup> The article was the first of a three-part series on human trafficking (HT).

Bagnall has worked in the anti-financial crime (AFC) space since 2007. He took leadership roles in three mid-size banks and one large bank, focusing on building and enhancing anti-money laundering (AML)/counter-terrorist financing, sanctions and fraud programs covering technology and analytics, risk assessments, high-risk customer management, training, exam/audit management and much more. He has extensive experience working with industries such as money services businesses, third-party payment processors, prepaid cards and merchant acquirers. In addition, he has led a collaborative initiative on behalf of banking peers to develop a new financial intelligence solution to change the paradigm of AFC program innovation, risk mitigation and intelligence sharing since 2020. He joined Quantexa in 2021 and as a solutions director, his work in the anti-HT field is focused on leveraging data and technology.

Bagnall is the regular contributor to the *Back to the Basics* column on ACAMSToday.org, has authored many articles for ACAMS Today and has worked with ACAMS on white papers, webinars and certification development programs.

Crowe is currently the senior vice president of Global Financial Investigations and Intelligence at Citibank. Prior to joining Citibank, Crowe served as the director of the strategic initiative on financial systems at Polaris, a U.S.-based nonprofit organization that is committed to the fight against



Chris Bagnall, CAMS-FCI



Sara Crowe

sex and labor trafficking. As strategic initiatives director, Crowe, who worked at Polaris for 12 years, was the head of Polaris’s financial intelligence unit (FIU), conducting in-house research and collaborating with financial institutions, law enforcement and HT survivors to detect HT operations through criminals’ financial footprints, to alleviate the burden placed on victims to testify in court, and to expedite financial restitution for trafficking victims—all in an effort to lessen the profitability of HT and make traffickers accountable for their crimes. Crowe also worked on financial inclusion endeavors to promote the financial resiliency of HT survivors and other vulnerable groups, encouraging businesses to adopt responsible financing practices and incorporate stronger protections for their workers. Crowe also serves as a member of the advisory board for the Finance Against Slavery and Trafficking Initiative. Crowe received a bachelor’s degree in political science and government from Wake Forest University and a master’s degree in conflict resolution from Georgetown University.

**ACAMS Today (AT):** Your article, “Understanding Human Trafficking,” clearly struck a chord with readers. What inspired you to write the article and what do you hope readers learned from it?

**Chris Bagnall (CB):** Since I began writing for ACAMS, I have always wanted to write on the HT topic. It was Sara who ultimately inspired me to put pen to paper. By chance, Sara and I attended an inaugural AML Partnership Forum in

Washington, D.C., in 2022. We were discussing ACAMS Today’s *Back to the Basics* column and I asked if she had an interest in writing an article. Sara mentioned she had a vision for an HT article series that fit the goal of the column (i.e., simplifying complex topics down to the basics). After saying something along the lines of, “Well, let’s do it,” we were off to the races.

Our goal for the article and the entire series was to drill down to the most important elements of what a reader should know about the complex and broad topic of HT. Should the reader wish to go deeper, we wanted to provide the most relevant resources on which the reader should focus. Ultimately, we wanted the reader to walk away with a clear understanding of HT.

We have received such amazing feedback from the financial crimes community on the article series. One of the best outcomes has been inspiring and enabling others to join the fight. There is no better outcome than that.

**Sara Crowe (SC):** At Polaris, I had been working with AML professionals for several years on the issue of HT and we were making great progress, but I wanted to get the entire industry involved. Every time someone new joined the effort, I was thrilled that participation was expanding, but I also found that there were varying levels of familiarity with the subject. I frequently had to go “back to basics” to make sure we were all working from a shared baseline level of knowledge. Having this conversation again and again, I had come to understand the most common gaps in knowledge or misconceptions. When Chris told me about his concept for the *Back to the Basics* column, I thought it was an incredible opportunity to establish that shared foundation across the industry. If we’re all on the same page, we can really accelerate our progress and innovation in this area.

**AT:** What was your motivation for wanting to write for ACAMS Today?

**CB:** Reading and writing are a passion of mine and I will read any topic (e.g., astronomy, history) in any medium. My first exposure to ACAMS Today was at the start of my career. In fact, I still have every ACAMS Today magazine that has been issued. I have always been inspired by those who take time out of their busy lives to educate the AFC community, and I wanted to do my part. It wasn't until I got to know Karla Monterrosa-Yancey and the ACAMS Today team that the interest turned into motivation, which turned into action.

My first article, titled "Exam-Ready AML and Sanctions Programs,"<sup>2</sup> was inspired by my experience at a bank considered higher risk by the Office of the Comptroller of the Currency due to a customer base that included check cashing businesses, prepaid cards, third-party processors and more, as well as products/services, such as trade finance and merchant acquiring. We spent a lot of time with our examiners showcasing our great financial crimes program, ultimately resulting in our program being considered one of the strongest. I wanted to share this experience with the financial crimes community.

The success of publishing this article opened the door for me to write numerous articles, many in collaboration with so many other brilliant financial crime prevention professionals over the past several years.

**SC:** As the Polaris FIU director, my goal was to educate AML professionals and motivate them to get involved. There is no better platform to reach AML professionals than ACAMS Today. Like Chris, I love to write. While I've done a lot of public speaking, I prefer to communicate in writing. I am really a true nerd.

**AT:** What advice would you give to other AFC professionals who would like to write for ACAMS Today but have yet to take the first step?

**CB:** When I have had an opportunity to provide advice to those interested in writing for ACAMS Today, I always try to provide three key pieces of advice:

- Start with the topic you are most passionate about and comfortable with. This doesn't mean you shouldn't take a chance on something new, but getting that first article published, where you can share your knowledge and experience, will go a long way. Even if others have written on the same topic, that doesn't mean you shouldn't. We all have different experiences and sharing those experiences is how we grow.
- Start small. I've written plenty of 2,000+ word articles and that can be daunting even for seasoned authors. But the ACAMS Today team is just as happy to publish a 400-word article. Part of the reason why the *Back to the Basics* column was established was to provide authors an avenue to write smaller, succinct articles. Leverage mediums like this to get started.
- Don't take no for an answer. One factor that impacted my ability to write early in my career was the approval process at the banks I worked for. Before writing anything, make sure there are no issues or limitations on writing content for ACAMS Today. If you are told you can't write, don't be discouraged. It is your career and anything important is worth fighting for.

The ACAMS Today team is amazing in their support of new and seasoned authors. Don't be afraid to reach out and ask how to get started!

**SC:** I would say to team up with Chris Bagnall because he is a wonderful writing partner and really guided me through the process. But if you can't do that, the first step is creating a clear concept of what you want to say. Think



about what your unique contribution to the field can be. Maybe you had this idea in the back of your mind that you haven't heard anyone else talking about. Maybe there is a type of case you have handled again and again, and you've become the resident expert on that typology. Or you've come up with a unique solution you've found to a common problem. Whatever it is, be clear on your concept. Next, while I won't literally advise you to "write drunk, edit sober," I will tell you not to hold back on your first draft. Just focus on getting your ideas on paper and go back to clean them up later. For me, the hardest part is always the editing phase. I think it was Mark Twain who said, "I didn't have time to write a short letter, so I wrote a long one instead." I was lucky on this series of articles that I had Chris to keep me in check because if it were up to me, I would have written a tome. Ultimately, I think our articles are powerful because they are so highly digestible. Your end result should be something someone will actually read, and let's be honest, we're all busy. The more concise the article, the more likely people will read it.

**AT:** How did you become involved in the fight against HT?

**CB:** My first real-world exposure to HT came approximately 10 years ago while I was in banking. We would routinely identify potential sex trafficking using prepaid payroll cards. In fact, the most common risk we reported through our prepaid payroll card portfolio was HT. It was during this time that we engaged with Polaris, where I met Sara. Our teams worked closely, sharing the new and emerging HT risks. Our efforts were rewarding and motivating. I was determined to continue finding a way to do more. Since then, Sara and so many others, including Aaron Kahler of the Anti-Human Trafficking Intelligence Initiative and Silvija Krupena of RedCompass Labs, have inspired and supported my efforts to play a role in tackling this abhorrent crime.

**SC:** My start in the anti-trafficking field is not a particularly noble story. In all honesty, I finished grad school at the height of the recession and needed a job. I started casting my net wider and wider in my job hunt. One day, I found a part-time role working on the National Human Trafficking Hotline operated by Polaris. I've always been a good listener—I am always that person with whom people feel comfortable confiding. I remember having a moment of clarity during which I thought, "I think I could be good at this, and maybe I could help some people while I look for my 'real job'." I started working overnight and weekend shifts. Honestly, the hours were so grueling and the subject matter was so intense. I'd finish a 10-hour adrenaline-filled shift of talking to people during the worst moments of their lives at 8 a.m. and have to be back for another shift at 2 p.m. that same day. But the work was also so compelling—I couldn't walk away. One thing led to another and instead of it being a part-time gig for a year while I found my career, it became my career, and I spent 12 years in different roles at Polaris.

**AT:** What would you recommend for professionals looking to get more involved in anti-HT efforts?

**CB:** One piece of advice I live by, although I know it isn't always the easiest for everyone, is to just ask. You will not hear the word "no" from anyone who has dedicated their career or has any involvement in the anti-HT space. If the individual can't directly help you, they will point you in the right direction. There are so many ways to get involved, so be open to opportunities presented to you. My journey has taken me down many paths I didn't expect, leading to several opportunities and interactions with amazing individuals. We each play a part, no matter how big or small, in tackling HT. I implore everyone to find their role.

**SC:** First, I would ask everyone to make sure they read all three articles in our series. We worked hard to distill broadly key information about HT, sex trafficking<sup>3</sup> and labor trafficking<sup>4</sup> down into a digestible format and after 12 years of focus on this topic, I can tell you this is really the key information you need to know to get started. Secondly, think about where you can contribute right now. No one person is going to be able to solve this incredibly complex issue, but everyone can do something to move the ball forward. Share these articles with your team and ask your colleagues if anyone would like to discuss them with you. Create an HT-specific data mining project at work. Visit [globalmodernslavery.org](https://globalmodernslavery.org) to find anti-trafficking organizations in your area and see if they have volunteer opportunities. **AT**

Interviewed by: ACAMS Today editorial, ACAMS, [editor@acamstoday.org](mailto:editor@acamstoday.org)

<sup>1</sup> Chris Bagnall and Sara Crowe, "Understanding Human Trafficking," ACAMS Today, April 19, 2022, <https://www.acamstoday.org/understanding-human-trafficking/>

<sup>2</sup> Chris Bagnall, "Exam-Ready AML and Sanctions Programs," ACAMS Today, March 30, 2021, <https://www.acamstoday.org/exam-ready-aml-and-sanctions-programs/>

<sup>3</sup> Chris Bagnall and Sara Crowe, "Understanding and Identifying Sex Trafficking," ACAMS Today, May 20, 2022, <https://www.acamstoday.org/understanding-and-identifying-sex-trafficking/>

<sup>4</sup> Chris Bagnall and Sara Crowe, "Understanding and Identifying Labor Trafficking," ACAMS Today, July 29, 2022, <https://www.acamstoday.org/understanding-and-identifying-labor-trafficking/>

## 2023 ACAMS Rising AFC Professional of the Year

### Toms Platacis: Adapting and advancing

**M** meet the 2023 winner of the *ACAMS Rising AFC Professional of the Year Award*, Toms Platacis, Certified Anti-Money Laundering Specialist (CAMS). Platacis has over six years of experience in anti-financial crime (AFC), and since September 28, 2023, has been the head of the Latvian financial intelligence unit (FIU). His prior role was deputy head of the Latvian FIU, leading the strategic analysis and cooperation coordination division responsible for the implementation of public-private partnerships.

In addition, Platacis is a board member of the ACAMS Baltic Chapter. He also contributes to the Financial Action Task Force (FATF)/MONEYVAL peer reviews as an evaluator, and as head of Latvia's delegation to MONEYVAL and FATF. Platacis earned his master's degree in law from the University of Latvia. His legal background combined with his AFC experience have enabled him to share valuable content through his contributions to the *ACAMS Today* magazine and as a speaker at ACAMS symposiums.

**ACAMS Today (AT):** *What areas of AFC are you focused most on improving?*

**Toms Platacis (TP):** My overall goal is to restore Latvia's reputation in AFC. We have done a major overhaul of the entire anti-money laundering/counter-terrorist financing system during the last five years to ensure that we can efficiently protect Latvia against any potential abuse of the financial system. This is one of the reasons why Latvia has applied to be among the first countries to be evaluated under the sixth MONEYVAL evaluation round.

In my current role (the core functions of the FIU), my primary focus lies in enhancing the quality of suspicious transaction reports (STRs). I believe that the efficiency of AFC measures and the overall resilience of the AFC system strongly depend on the accuracy and relevance of STRs. By improving the quality of STRs, I aim to enhance the FIU's ability to detect and prevent potential financial crimes and contribute significantly to our overall risk mitigation efforts.



Another key area of my focus is digital transformation, with a particular focus on cutting-edge technologies, such as artificial intelligence (AI) and machine learning. I strongly believe that in an increasingly complex financial landscape, the integration of AI and machine learning tools in daily work is a prerequisite. In the area of AFC, innovations are business enablers and even drivers that empower us to analyze large amounts of data with unprecedented speed and accuracy. In addition, digital transformation not only enhances the efficiency of our AFC systems and processes but also enables us to respond swiftly to emerging new risks and, therefore, strengthens the FIU's overall capabilities to protect our financial system against financial crime. We have already piloted several new initiatives, such as the "black box" and OpCEN (an enhanced operational public-private partnership model), and the early results are positive.

And last but not least, I am a strong believer in international cooperation in the area of AFC. That is the reason why I try to be as active as possible in the international arena. I am a regional representative of the Egmont Group Europe I Regional Group; a MONEYVAL assessor; a board member of the ACAMS Baltic Chapter; and a member of two ACAMS task forces. And even then, I am keen to expand my role and contribute even more.

**AT:** *From your experience, what tools or resources are most instrumental in staying current with emerging financial crimes?*

**TP:** In my experience, staying current with emerging financial crimes demands an approach that involves a variety of tools and resources. First, I consider that

professional networks play an important role. I am a strong believer in the Egmont Group, in our "superpower" of exchanging and sharing information, but even beyond that, engaging with my peers nationally and internationally, regulatory bodies and law enforcement agencies is extremely important to understand the risks, the outlook, the strengths and the weaknesses of the AFC systems. It is your network that can help you stay one step ahead in the battle against financial crime.

International events and conferences are equally essential. I try to attend as many as possible and I try to contribute as a speaker as often as possible. These platforms bring together experts and thought leaders from across the globe. Since financial crimes become more and more global, interconnected and cross-border, our response should be even better and with closer collaboration. This is why I consider such events instrumental in shaping our AFC strategies and ensuring they are indeed effective.

Last but not least, effective communication, continuous learning and exchange of information within and outside the organization is a must.

**AT:** *What are the parts of your career that you have enjoyed the most?*

**TP:** I was fortunate to be the acting head of the FIU last summer when my country and FIU Latvia were hosting the 28th Egmont Group Plenary in Riga, which was the first in-person meeting since 2019. It was an immense pleasure to be able to finally re-shake hands with all our international partners. In addition, everyone on my team and I took great pride and responsibility in hosting over 400 delegates from


125 countries in our hometown. We wanted not only to have a productive and meaningful event but also to show a little glimpse of our wonderful country and culture. And I believe we did this! It was a real team effort and I can only recommend everyone to go through this experience!

**AT:** *What is the most helpful piece of information you have learned that has helped you advance in your career?*

**TP:** I would say, first, it is enthusiasm that has been my driving force. My willingness to really understand the complexities of the world of financial crimes, my willingness to learn and discover, coupled with the passion to make a difference. I am certainly not somebody who wants to go about "business as usual." I want to strive. I want to solve difficult things. I want us (the FIU) to be among the best.

Second, I can see that the digital world is our future. Sometimes, it is difficult to see where exactly it will take us, but one thing is clear—it provides huge opportunities. This is why I want our FIU to be an agile organization, one that can quickly adapt and respond to the changing world, embrace new technologies and prioritize collaboration and flexibility.

**AT:** *What advice would you offer to AFC professionals wanting to go above and beyond in their careers?*

**TP:** Easy! Stay persistent, stay curious and never stop learning. Finally, work hard. And by hard, I mean harder than anyone else. 

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



## 2023 ACAMS AFC Professional of the Year

### Nicholas Schumann: Building a positive work culture

**A**CAMS Today talked to the 2023 ACAMS AFC Professional of the Year recipient, Nicholas Schumann, who is the U.S. head of Financial Crime Framework, senior vice president at HSBC. In his current role, he is responsible for helping guide HSBC's participation in public-private financial information sharing partnerships in the U.S. to support intelligence-led financial crime risk management. Before assuming this role, Schumann served as deputy director for HSBC's financial intelligence unit in the U.S., overseeing a team that analyzed complex, multi-jurisdictional financial crime threats. Prior to joining the bank in 2015, he worked at the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence for almost seven years. Schumann also holds the rank of Major in the U.S. Army Reserve and has been deployed to Kuwait and Iraq. A regular contributor to ACAMS Today, Schumann is also co-chair of the ACAMS South Florida Chapter.

**ACAMS Today (AT):** Congratulations, Nick! What were some of the specific high points in your career during the past year?

**Nick Schumann (NS):** Many thanks—being named the ACAMS AFC Professional of the Year is an amazing honor and quite humbling. As far as recent career high points, this award is certainly at the top of the list. Earlier this year, I was also lucky to have been named an HSBC "Culture Hero," which recognizes colleagues' contributions to building a positive work culture and supporting diversity and inclusion efforts. Through HSBC's Employee Resource Group (ERG) network, I am heavily involved in efforts to support military veteran transition efforts to the civilian sector, and this includes anti-financial crime (AFC) roles, of course.



**AT:** As an active member of ACAMS and co-chair of the ACAMS South Florida Chapter, how important would you say ACAMS has been to your career?

**NS:** I'm proud to say that I have been an ACAMS member and earned my Certified Anti-Money Laundering Specialist (CAMS) designation in 2009, so I am coming up on almost 15 years of affiliation with ACAMS. I remember initially seeking membership after joining the U.S. Department of the Treasury's intelligence office. Although I was not new to the intelligence community at the time, I was certainly new to the financial crime space and gaining membership and getting certified through ACAMS absolutely helped me improve my AFC overall knowledge base. Fast forward to 2021, when I joined the South Florida Chapter Board. I had just come off 14 months of active duty leading U.S. Southern Command's (Southcom's) Counter-Threat Finance Branch in Miami, Florida, and was returning to HSBC in a civilian capacity, and very thankfully able to stay in South Florida. I was looking to strengthen my local AFC network and find a way to give back; joining the South Florida Chapter Board made this possible.

**AT:** Why should members of the AFC community who are not yet ACAMS members join ACAMS? How would membership benefit their careers?

**NS:** AFC professionals, or aspiring ones, should consider membership to learn about and stay up-to-date on emerging financial crime topics such as the importance of public-private partnerships, increased concerns with environmental crimes such as illegal logging, as well as the increasingly important role of technology (such as artificial intelligence) in combating financial crime. Membership provides numerous learning opportunities and strengthens career development by enhancing your professional network. Chapter engagement also helps in both regards and there are many chapters located throughout the world that members can join and support. It's worth noting that—as with most things—you will get what you put into your membership. I know that's been my experience.

**AT:** During your career, you served in the U.S. Army Reserve, the U.S. Department of the Treasury and then in the private sector at HSBC. How has serving in the military and both the public and private sectors shaped your career and your life in general?

**NS:** I have thoroughly enjoyed having the opportunity to serve my country through both civilian and military roles and would strongly encourage folks to consider government service. Within the public

sector, I was able to work alongside dedicated people committed to helping keep our nation and local communities safe from harm. In the private sector, I have found and been able to work closely with colleagues equally committed to serving our communities and keeping them safe. The inputs might be different across the public and private sectors, but the outputs are generally the same: Doing the right thing in the right way. Bringing a public sector perspective to the private sector—and vice versa—is incredibly valuable and offers some important insights you might not otherwise gain.

**AT:** You are heavily involved in Veterans on Wall Street (VOWS). Could you tell us more about VOWS and how members could contribute to this organization?

**NS:** VOWS is an initiative dedicated to honoring former and current military personnel by facilitating career and business opportunities in the financial services industry (and more broadly across the private sector).<sup>1</sup> VOWS events are held around the country throughout the year and directly supported by the VOWS strategic philanthropic partner, the Bob Woodruff Foundation (BWF).<sup>2</sup> For example, by the time this article is published, two major VOWS symposia will have been held in New York City and Miami, timed with Veterans Day. If anyone is interested in learning more and getting involved, either on an individual basis or as an organization, I would encourage reaching out directly to BWF through their website. **AT**

Interviewed by ACAMS Today editorial, ACAMS, Miami, FL, USA, editor@acams.org

<sup>1</sup> Veterans on Wall Street homepage, <https://veteransonwallstreet.com/>

<sup>2</sup> Bob Woodruff Foundation homepage, <https://bobwoodrufffoundation.org/>

**Bringing a public sector perspective to the private sector—and vice versa—is incredibly valuable and offers some important insights you might not otherwise gain**

## 2023 ACAMS Chapter of the Year

### ACAMS Carolinas Chapter: Creating opportunities to build relationships



Pictured left to right are Nicolas Khouri, Tyler Reynolds, Peter Wild, Eddie Robinson, Lisa Grigg and Robert Goldfinger.

**T**he recipient of the 2023 ACAMS Chapter of the Year Award is the ACAMS Carolinas Chapter. The chapter hosted various successful events with high attendance rates and has amassed a large social media presence and following, motivating ACAMS members to join their local chapters. Through their educational events, anti-financial crime (AFC) professionals were able to network with like-minded professionals to continue their learning journey in the ever-evolving AFC field. The ACAMS Carolinas Chapter board spoke with *ACAMS Today* about their accomplishments and the success of their chapter.

**ACAMS Today (AT):** What was your greatest accomplishment in 2023? What do you have in store for 2024?

**ACAMS Carolinas Chapter (ACC):** Overall, our biggest accomplishments in 2023 were getting back to a full programming schedule and making a key leadership decision for the future. We continued our flagship event—the AML and OFAC Symposium—and delivered 14 events. We are certainly proud of our programming, but we also spent time refreshing our board membership, ensuring that we migrated leadership positions, and most notably, named Nicolas Khouri and Beth Herron as our next chapter co-chairs. Jim Arndts and Megan Hodge are thrilled to have both Nicolas and Beth step into the co-chair positions in 2024 and are certain they will continue the chapter's positive momentum.

**AT:** What was your most popular event in 2023, and what were the main topics discussed?

**ACC:** The Carolinas Chapter aims to provide diverse and impactful programming to ACAMS chapter members throughout North and South Carolina. The board of the Carolinas Chapter provides frequent programming to ACAMS members and potential members. In the past 12 months, the chapter has delivered 14 different sessions to over 1,800 attendees in forums ranging from daylong symposiums with topics relevant to the financial crimes landscape to member appreciation events.

Our most popular event in 2023 was “FinCEN National Priorities—A Tactical Approach,” hosting 369 attendees. On June 30, 2021, the Financial Crimes Enforcement Network announced the first set of government-wide anti-money laundering (AML)/counter-terrorist

financing priorities, as required by the Anti-Money Laundering Act of 2020. Our panel of experts shared how their institutions have reacted to those priorities and what steps they took since these were announced. Our experts shared tactical and strategic steps as well as best practices on what to do while waiting for additional guidance.

Our second most popular event in 2023 was the “2023 AML and OFAC Symposium,” which had 234 attendees. This event was the ACAMS Carolinas Chapter's third symposium, which offered a full day of education that explored hot topics, best practices and networking opportunities. Topics covered included the Bank Secrecy Act officer round table, organized retail crime, fraud, governance to accelerate innovation, sanctions, human trafficking and a keynote from David Chenkin, managing partner and chair of Government Investigations, White Collar Defense and Anti-Money Laundering Group at Zeichner Ellman & Krause LLP.

**AT:** You have an active presence on LinkedIn, in addition to running a page for the Carolinas Chapter. What should members be looking for on these pages?

**ACC:** We try to reach out to members and future members where they are most active. By sharing across email, LinkedIn and our website, we hope to capture a broad group of AFC professionals in our area to ensure their participation in our educational and networking opportunities. We also recognize that, at times, schedules do not allow participation. The event blog available on our website is a resource where members can access summaries and key takeaways from prior events.

**AT:** What motivates you to continue hosting events and educating AFC professionals?

**ACC:** Our board comprises passionate professionals who believe we are all more successful at combating financial crime when we share knowledge. Creating opportunities for people in our market to build their professional network further amplifies the impact beyond the events themselves. We also recognize that the AFC space is continuously evolving, creating a need for a platform that enables established and emerging thought leaders to share their innovative ideas, practical advice and future projections.

**AT:** What recommendations do you have for other rising chapters?

**ACC:** Our chapter is continuously adapting and maturing as we “learn by doing.” Chapters are run by volunteers, and it is unlikely that your board members are experts in marketing, event planning, programming, etc.—but a board member willing to jump in and take on the challenge can make a huge impact! Take the time to take note of successes and opportunities for improvement so that you can better serve your members as you mature.

Programming is critical to the success of the chapter. We have found that focusing on case studies and real-life examples has been beneficial to our members. Events that have actionable takeaways receive the best feedback.

And finally, have fun! Working in AFC is a rewarding but demanding career. Get creative about networking, volunteering and other opportunities for members to build relationships with each other. [AT](#)

Interviewed by ACAMS Today editorial, ACAMS, Miami, FL, USA, editor@acams.org

## THE EVOLUTION OF MONEY LAUNDERING/ TERRORIST FINANCING IN FILM AND TELEVISION

**“W**hat do you do for work?” This is a straightforward question but one that can cause anxiety and dread to anti-financial crime (AFC) professionals. Financial crime risk management and the work we do to protect the financial system do not roll off the tongue over canapes and cocktails.

However, financial crime is having a popular culture moment where money laundering schemes are plot points. For me, it is an intersection of my two geekdoms: Film/television and financial crimes. This article will outline financial crime typologies presented in film and television and similar anti-money laundering (AML) typologies/red flags seen in real life examples. Spoiler alert: Life is stranger than fiction.

## Timeline of financial crime in film and television

### 1930s:

#### Organized crime and the mob accountant

Films in the 1930s depicted mob activities such as bootlegging, protection rackets and bribery. A mob accountant had a starring role in tracking the inflows and outflows. In the film *The Untouchables* (1987), the mob account/"bookkeeper" plays a critical role in identifying bribery payments and the sources of illicit funds. The bookkeeper role is so important that the Untouchables team recruits an accountant to translate the ledgers.

### 1970s:

#### Drug trafficking organizations

In the 1970s, the drug trafficking stories were primarily set in High Intensity Drug Trafficking Areas/High Intensity Financial Crime Areas (HIDTA/HIFCA). Two film examples are the *French Connection* (1971) and *Scarface* (1983), set in New York City and Miami, respectively. In both films, narcotics are being imported to the U.S. through international drug trafficking organizations.

### 1990s:

#### Proliferation and terrorist financing

The films in the 1990s depict terrorist financing activities as well as the proliferation of weapons of mass destruction. In the film *True Lies* (1996), the terrorist cell uses an antiques dealer as a front to carry out illicit activities.

### 2000s to today:

#### Rise of the money launderers

In the current era, money launderers and their associated techniques are at the center of the storytelling. The two popular examples are *Ozark* and *Breaking Bad*. At the center of each story, there is a family man who uses a unique set of skills to get his family involved in illicit activities and later to try to protect his family from criminal organizations. In *Ozark*, the Byrd family begins laundering money for a Mexican drug cartel via cash businesses in a resort area,

while *Breaking Bad* tells the story of a terminally ill high school chemistry teacher who begins cooking the infamous "blue meth." The product is so successful that the protagonist and his wife are overwhelmed by the volume of cash.

These television programs and movies present red flags that can help financial crime professionals identify potential suspicious activity. Some of these actions may include:

- Know your customer
- Understanding the risks posed to your organization
- Negative news and other relevant intelligence

## Case study one: *Sons of Anarchy* (2008–2014)<sup>1</sup> and *Mongols Motorcycle Club*

**Logline:** "A biker struggles to balance being a father and being involved in an outlaw motorcycle club."<sup>2</sup>

**Fictional financial crimes:** Bribery/corruption, drug trafficking, transnational criminal organizations

**Fictional red flags:** Unsourced cash

**Real world counterpart:** Tennessee Mongols Motorcycle Club

- Distributed more than 50 pounds of methamphetamine
- Committed violent acts, including kidnappings, assaults and murder

— **Case outcome:** The six defendants each sentenced to life in prison<sup>3</sup>

— **Potential AML red flags:** Negative news, source of funds and HIDTA/HIFCA locations



IN THE CURRENT ERA,  
MONEY LAUNDERERS  
AND THEIR ASSOCIATED  
TECHNIQUES ARE  
AT THE CENTER OF  
THE STORYTELLING

## Case study two: *Claws* (2017–2022)<sup>4</sup> and *Pill Mill Granny*

**Logline:** "A look at the life and crimes of five women who work at a Florida nail salon."<sup>5</sup>

**Fictional financial crimes:** Bribery/corruption, drug trafficking, transnational criminal organizations

**Fictional red flags:** Smurfing deposits, structuring and cash-intensive businesses (nail salon and casino)

**Real world counterpart:** Sylvia Hofstetter

- 11 million opioid tablets distributed
- \$360 million street value
- Maintained three pain clinics
- **Case outcome:** The defendant (Sylvia Hofstetter) was sentenced to more than 33 years in prison and required to pay \$3.6 million in restitution<sup>6</sup>
- **Potential AML red flags:** Source of funds and wealth, luxury purchases

## Case study three: *Dope* (2015)<sup>7</sup> and dark web online marketplaces

**Logline:** "Life changes for Malcolm, a geek who is surviving life in a tough neighborhood, after a chance invitation to an underground party leads him and his friends into a Los Angeles adventure."<sup>8</sup>

**Fictional financial crimes:** Bribery/corruption, cybercrime and drug trafficking

**Fictional red flags:** Nonprofit organization abuse

**Real world counterpart:** Ross Ulbricht

- Dark web marketplace founded on libertarian values
- Started to sell magic mushrooms
- Expanded to other illicit activities, including drugs, weapons, organ harvesting and murder
- Over \$1 billion in bitcoin transactions
- **Case outcome:** The defendant (Ross Ulbricht) sentenced to life in prison without parole<sup>9</sup>
- **Potential AML red flags:** Purchases for virtual private networks, online storage and no apparent source of wealth

## Conclusion

Today, when I am asked the dreaded question, I give a "choose your own adventure" response with "Would you like the truth or a lie?" I have found most people want both, and it starts out with the question "Have you seen..." then becomes a real-world AFC discussion. With so many AFC typologies touching on crimes that have a real impact, people will share their experiences or observations with front businesses, corruption, scams, elder abuse, human trafficking or Paycheck Protection Program loan activity. The anecdotes are relevant and applicable to my AFC work to "get into the mind" of the bad actor and see examples of how these typologies and red flags can play out in real life.

Not every film or television show "gets it right." Perhaps this is how *Grey's Anatomy* or *Law & Order* makes doctors and lawyers feel. But for the eagle-eyed financial crime professional, there are opportunities to observe and identify potential red flags encountered in real life. **AT**

Aminah Harris, CAMS, CFE, NJ, USA,  
aminah.harris@gmail.com

<sup>1</sup> "Sons of Anarchy," *IMDB*, <https://www.imdb.com/title/tt1124373/>

<sup>2</sup> *Ibid.*

<sup>3</sup> "Six Mongols Motorcycle Club Members Found Guilty of Racketeering Conspiracy, Including Murder," *U.S. Department of Justice*, September 19, 2022, <https://www.justice.gov/opa/pr/six-mongols-motorcycle-club-members-found-guilty-racketeering-conspiracy-including-murder>; "Members of Tennessee Mongols Motorcycle Club charged in woman, man's gruesome murder," *Fox17*, September 19, 2022, <https://fox17.com/news/local/members-of-tennessee-mongols-motorcycle-club-charged-in-woman-mans-gruesome-murder-clarksville-gangs-crime-alertnest>

<sup>4</sup> "Claws," *IMDB*, <https://www.imdb.com/title/tt5640558/>

<sup>5</sup> *Ibid.*

<sup>6</sup> "Pain Clinic Owner Sentenced for Role in Operating Pill Mills in Tennessee and Florida," *U.S. Department of Justice*, October 21, 2020, <https://www.justice.gov/opa/pr/pain-clinic-owner-sentenced-role-operating-pill-mills-tennessee-and-florida>; Robert Holder, "Judge sentences Knoxville pill mill operator to more than 33 years in prison, forfeiture of \$3.6 million," *WATE.com*, October 21, 2020, <https://www.wate.com/news/local-news/judge-sentences-knoxville-pill-mill-operator-to-more-than-33-years-in-prison-forfeiture-of-3-6-million/>; Hayley Fowler, "Grandmother's pill mills made millions in Tennessee, feds say. She's going to prison," *The Charlotte Observer*, October 22, 2020, <https://www.charlotteobserver.com/news/nation-world/national/article246637503.html>

<sup>7</sup> "Dope," *IMDB*, <https://www.imdb.com/title/tt3850214/>

<sup>8</sup> *Ibid.*

<sup>9</sup> Nick Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road*, 2017.



# Intelligence-driven compliance controls

**“T**he fate of the nation well may rest on accurate and complete intelligence data which may serve as a trustworthy guide ... in a troubled world where so many forces and ideologies work at cross purposes.”<sup>1</sup>

On Saturday, October 7, 2023, the Gaza-based terrorist group Hamas commenced a large-scale attack on Israel, launching thousands of rockets and gunning down civilians just after daybreak. According to Israel’s Foreign Ministry,<sup>2</sup> since the initial attack, Hamas has killed approximately 1,200 Israelis. Innocent lives have now been lost on both sides of the escalating war. We mourn the loss of innocent life wherever it happens. And those whose profession and mission it is to detect and prevent illicit finance from wreaking havoc on communities and financial systems will no doubt turn a renewed and sharpened focus to the entities and methods that fund these atrocities. How can we do that and be more effective than in times past?

In reading through the news coverage and trying to unpack the senselessness, a report emerged

regarding what may have been known about the attack before that fateful Saturday. According to a CNN article, “The [U.S.] intelligence community produced at least two assessments ... of an increased risk for Palestinian-Israeli conflict in the weeks ahead of Saturday’s seismic attack on southern Israel, according to sources familiar with the intelligence.”<sup>3</sup> The article goes on to state that the assessments did not necessarily offer specific details on the scale, scope or tactics of the attack, but that the risk of escalation was rising.

Then came this striking statement from the article: “‘The problem is that none of this is new,’ said one of the sources familiar with the intelligence. ‘This is something that has historically been the norm.... I think what happened is everyone saw these reports and were like, ‘Yeah of course. But we know what this will look like.’”<sup>4</sup>

In other words, there was a general agreement and acknowledgment of the type of risk itself (i.e., Hamas as a threat to attack Israel) but not a precise understanding of the magnitude of that risk.

In the AFC space, there is a general acknowledgment of the most prominent risks we all face. We know fraud and cybercrime is a systemic problem. We know pig butchering scams are on the rise. We know drug cartels and transnational organized crime networks exploit our financial system across the globe to launder their ill-gotten gains. We know Russian oligarchs use shell companies in various jurisdictions to evade sanctions. “None of this is new.”

But do we know, on a quantitative basis, the magnitude of each of those risks? How much volume each year stems from those bad actors, how is it changing over time, what specific venues and jurisdictions are being exploited, and how does illicit activity adapt to our countermeasures like sanctions designations? In the dollar-fiat context, we have estimated by think tanks, past suspicious activity reports, subject-matter expert anecdotes and targeted risk assessments that speculate on those questions. We then base the vast majority of our control environment decisions on those best approximations. However, there exists a risk that we may misjudge, wrongly assess or

*In the national security sector, intelligence is integral to every facet of decision-making, strategy formulation and threat mitigation*

completely miss the magnitude of each of those risks in our institutions, making it challenging to know how to tune our controls and surveillance, furthering the cat-and-mouse game instead of finding the endgame to these shared risks. As an industry, we need to raise the bar on the collection, use and programmatic incorporation of intelligence.

With respect to digital assets, there is an increased level of precision in the financial intelligence available. Crypto brings inherent risks, but it also brings the promise of greater intelligence that compliance professionals can leverage to make more accurate and timely decisions to detect and prevent illicit finance. The transparency and vast amounts of blockchain data, coupled with open-source intelligence and a threat-hunter mindset, collectively build a rich intelligence picture of the criminals' and terrorists' economic activity that targets our society and financial systems.

In the national security sector, intelligence is integral to every facet of decision-making, strategy formulation and threat mitigation. Former United States Director of National Intelligence Dennis Blair once testified that, "Nothing is more important to national security and the making and conduct of good policy than timely, accurate, and relevant

intelligence."<sup>5</sup> So too it should be said with AFC and illicit finance, where timely, accurate and relevant intelligence can drive more effective investigations that lead to actionable intelligence for law enforcement (LE), as well as more effective control decisions to better tailor your AML program to the exact risks your institution faces.

For instance, with blockchain intelligence, we can say a good deal of things about Hamas and their crypto funding operations.<sup>6</sup> We can also assess how effective OFAC's Tornado Cash sanctions designation was by observing the precise amount of flows and decreases in volume since OFAC's action. When criminal laundering patterns shift from one asset to another, we can tell you when that shift started, in what proportion, and where it may be going next. We can tell you the preferred asset and blockchain of bad actors at this moment. When a darknet marketplace gets shut down by coordinated international LE efforts, we can tell you what emerging marketplaces are filling their place and how quickly they are moving. As nation-state cybercriminals and money launderers switch tactics to evade detection, we can see what new patterns and venues they use to find new chokepoints for their operations.

Now, we do not mean to suggest that greater intelligence is the panacea to stopping events like brutal terrorism. Knowing the approximate funding amounts Hamas was receiving in crypto did not prevent the attacks. But there is little doubt that accurate and timely intelligence needs to play an increasingly larger role in the arsenal and toolkit of every compliance officer looking to stop criminal and terrorist networks. The role of intelligence in risk assessments, surveillance design, investigative leads and feedback loops has historically been underutilized. Intelligence-driven compliance controls will make it harder, costlier and riskier for groups like Hamas to move money and exploit our institutions, and blockchain intelligence is beginning to lay the groundwork for that future vision. [AI](#)

*Thomas Armstrong, TRM Labs, head of Compliance Advisory, San Francisco, CA, USA, [tom@trmlabs.com](mailto:tom@trmlabs.com), [in](#)*

<sup>1</sup> "Report by the Task Force on Intelligence Activities of the Commission on Organization of the Executive Branch of the Government," *United States Department of State*, May 1955, <https://history.state.gov/historicaldocuments/frus1950-55Intel/d220>

<sup>2</sup> Aaron Boxerman, "What We Know About the Death Toll in Israel From the Hamas-Led Attacks," *The New York Times*, November 12, 2023, <https://www.nytimes.com/2023/11/12/world/middleeast/israel-death-toll-hamas-attack.html>

<sup>3</sup> Katie Bo Lillis, Zachary Cohen, Alex Marquardt, et al., "US intelligence warned of the potential for violence days before Hamas attack," *CNN*, October 13, 2023, <https://www.cnn.com/2023/10/13/politics/us-intelligence-warnings-potential-gaza-clash-days-before-attack/index.html>

<sup>4</sup> Ibid.

<sup>5</sup> "Statement of Dennis C. Blair before The Senate Select Committee on Intelligence United States Senate, January 22, 2009," *Director of National Intelligence*, January 22, 2009, [https://www.dni.gov/files/documents/Newsroom/Testimonies/20090122\\_testimony.pdf](https://www.dni.gov/files/documents/Newsroom/Testimonies/20090122_testimony.pdf)

<sup>6</sup> "In Wake of Attack on Israel, Understanding How Hamas Uses Crypto," *TRM Labs*, October 10, 2023, <https://www.trmlabs.com/post/in-wake-of-attack-on-israel-understanding-how-hamas-uses-crypto>

# VISUALIZE YOUR ARTICLE HERE



**CONTRIBUTORS' GUIDELINES:**



**EDITORIAL CALENDAR:**



# WHY CHATGPT IS UNLIKELY TO REPLACE THE HUMAN FACTOR IN AML

**A**rtificial intelligence (AI) describes the development of computer systems that can perform tasks typically requiring human intelligence, such as learning, reasoning and problem-solving. AI has already been used across a multitude of industries' to improve daily life. It has been implemented in the health care industry to carry out more accurate diagnoses. In the food industry, AI develops methods to raise more perfect crops. In the banking industry, AI quickly processes loan applications.

As AI continues to develop into a powerful and accessible tool, society benefits from its wide-ranging applications. Since criminals—particularly financial criminals such as fraudsters, money launderers and terrorist financiers—tend to be early adopters of new technology, the work we all do in anti-money laundering/counter-terrorist financing (AML/CTF) has just become more difficult. Examples of technology being adopted by criminals range from using the dark web to buy and sell illegal goods,<sup>2</sup> to email phishing scams and recent internet-based pig butchering scams.<sup>3</sup>



### ChatGPT and AI overview

One such example of an accessible AI application is ChatGPT, a program created by OpenAI. ChatGPT is one in a series of natural language models<sup>4</sup> deployed by OpenAI. For a layperson, language models might be comparable to a supercharged autocorrect engine.<sup>5</sup> That is to say, ChatGPT does not really know anything, but it is able to relay a series of words that are generally associated with each other.

Most significantly for all of us in the compliance sector, ChatGPT does not check facts. To the contrary, at the bottom of the ChatGPT prompt screen, there is this disclaimer: “Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts.” Information provided by ChatGPT must be independently verified to be trusted. Overreliance on the accuracy of ChatGPT has already caused problems for legal professionals. One New York attorney was fined for submitting a legal brief that cited fictitious cases<sup>6</sup> compiled by ChatGPT, which has been known to invent cases or facts to cases.<sup>7</sup>

The authors asked ChatGPT about itself and found that someone or something, most likely a human, wrote what amounts to a disclaimer so broad as to reduce or eliminate the use for AI. In part, it reads, “ChatGPT sometimes writes plausible-sounding but incorrect or nonsensical answers.”<sup>8</sup> This disclaimer should be posted whenever text provided by ChatGPT is used, quoted or referenced in any form.

In short, ChatGPT uses machine learning algorithms to process and analyze data and generate responses to users’ inquiries that are accessible, friendly and often couched in the first person, i.e., “Yes, I can”<sup>9</sup> or “However, I should note.”<sup>10</sup>

This means that when users type a question into ChatGPT, it produces a conversational answer.

For example, when prompted to “Describe how to use ChatGPT to prevent money laundering schemes in the United States,” ChatGPT provided a list of ways it could be used to support a comprehensive AML program or regulatory compliance: “ChatGPT can aid in preventing money laundering schemes in the United States by providing real-time analysis of financial transactions, identifying suspicious patterns or activities, and offering guidance on relevant regulations and compliance measures. By integrating GPT-3.5 into financial monitoring systems, it can help identify red flags, potential money laundering activities, and suggest appropriate reporting steps to relevant authorities. Additionally, it can provide training and educational resources to financial professionals to enhance their understanding of evolving money laundering tactics and regulatory updates, thus contributing to a proactive approach in combating financial crimes.”<sup>11</sup>

Although it can be a helpful tool, ChatGPT will tell you that it is not a substitute for a comprehensive AML program, nor can it replace the human element.

### ChatGPT’s limitations

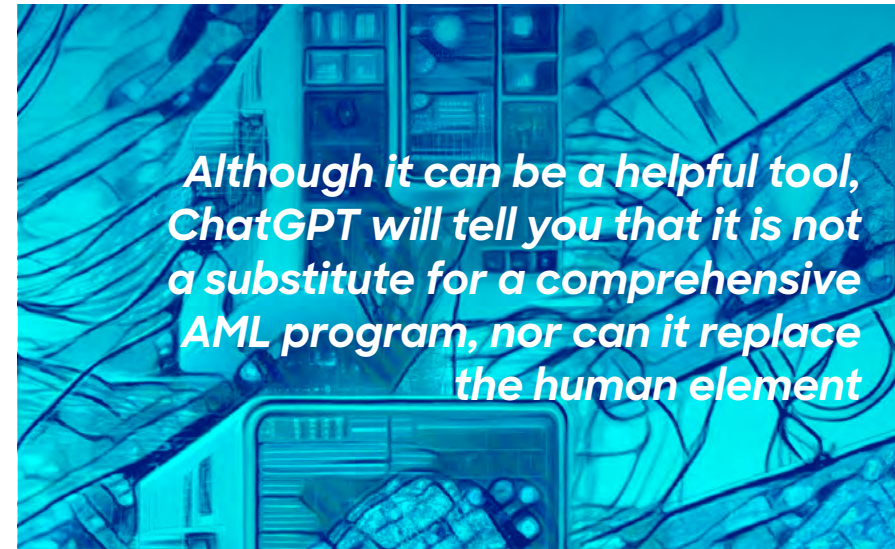
ChatGPT has flaws: For one, ChatGPT is only as good as the information it has been fed. It is the old story of garbage in, garbage out since ChatGPT is limited by the veracity of its source data. In addition, it reflects the views back to us that it picks up from its source data, but not the internet at large. Unlike search engines like Google that have access to the entire internet, ChatGPT in its present form is limited to the source data available at the time it was created (e.g., data

available up until September 2021). Further, AI is a reflection of societal knowledge and, therefore, is susceptible to the same things to which people are susceptible, such as sexism,<sup>12</sup> racial bias and political polarization. When you Google something, you are given multiple sources and it is up to you to trace what you want to use, from where the information is coming and who wrote it. When you ask ChatGPT something, you do not necessarily know who wrote it, let alone whether the information provided is accurate. This leads back to a flaw discussed above: ChatGPT has been known to make stuff up.

### Effect on the AML field and on criminals

ChatGPT can provide accurate answers to a variety of AML and Bank Secrecy Act (BSA)-related issues. Below are questions asked to ChatGPT and the range of responses vary in accuracy.

**Example:** In response to being asked, “What is the definition of a currency transaction report?” the following appeared: “A Currency Transaction Report (CTR) is a financial document required by the Financial Crimes Enforcement Network (FinCEN) in the United States, typically completed by financial institutions, which details any transactions involving cash amounts over a certain threshold (currently \$10,000) within a single business day. The report includes information about the transaction, the parties involved, and the purpose of the transaction, aiding in the detection and prevention of money laundering and other illicit activities.”<sup>13</sup>



**Analysis:** The response is pretty accurate, concise and helpful, and most importantly, it makes clear that the threshold for U.S. CTRs is over \$10,000, not \$10,000 or below, as many folks believe.

**Example:** Contrast the previous example to the response we received to the question: “What does section 314(b) of the USA PATRIOT Act say?”

“Section 314(b) of the USA PATRIOT Act encourages collaboration and information sharing among financial institutions, specifically with regard to detecting and preventing money laundering and terrorist financing. The section enables the sharing of information regarding individuals or organizations that may be involved in such illicit activities.

Here is a summary of the key points from Section 314(b) of the USA PATRIOT Act:

1. Information Sharing Authorization: Financial institutions are authorized to share information with one another or with associations of financial institutions regarding individuals, entities, organizations, or countries suspected of involvement in money laundering or terrorist activities.
2. Voluntary Sharing: The information sharing under Section 314(b) is voluntary, meaning that financial institutions are not mandated to share information, but they are encouraged to do so to enhance the collective effort to combat financial crimes.
3. Protection from Liability: Financial institutions that voluntarily share information in accordance with the provisions of Section 314(b) are protected from liability for such sharing and are deemed to be in compliance with privacy and confidentiality obligations.
4. Purpose of Sharing: The sharing of information is intended to help financial institutions identify and report potential money laundering or terrorist financing activities more effectively. By sharing insights and suspicions, institutions can collectively strengthen their ability to detect and prevent financial crimes.

5. Privacy and Confidentiality Considerations: While promoting information sharing, financial institutions must still maintain the privacy and confidentiality of shared information in accordance with applicable laws and regulations.

Section 314(b) was enacted to facilitate cooperation and collaboration among financial institutions, thereby improving the collective ability to identify and respond to suspicious activities related to money laundering and terrorist financing. It provides a framework for sharing relevant information while offering liability protections for those participating in good faith.”<sup>14</sup>

**Analysis:** The response is seemingly accurate, not particularly concise, and missing at least two key points: First, in order for a financial institution (FI) to participate, the FI must first register with FinCEN<sup>15</sup> and do so annually. There is no reference to this requirement in the ChatGPT formulation. Second, the FI may only share information with another FI registered with FinCEN.<sup>16</sup> In either case, failure to register or exchange information with a registered FI will cause the FI providing information to lose the safe harbor provided for in 314(b), which is one of the essential elements of that section.


One day, AI, like ChatGPT, may make it easier for criminals to conduct illegal activities. Criminals could create their own AI to simultaneously run thousands of scams at once or even bypass security and safety mechanisms put in place by organizations like OpenAI to prevent misuse of their proprietary systems or existing AI programs.

### Takeaways

1. You can use ChatGPT as a starting point but cannot rely on its accuracy. If you do not believe us, just ask ChatGPT! When asked, “Can I rely on the answers ChatGPT provides?” ChatGPT responded: “While ChatGPT can offer helpful information and suggestions, it’s crucial to exercise caution and verify the accuracy and reliability of the answers provided, especially for critical or important decisions. Always cross-reference the



information with credible sources and consult professionals when needed to ensure accuracy and appropriateness for your specific situation.”<sup>17</sup>

2. Google, Bing, Yahoo! and other search engines are not only useful but are required.
3. The absence of source documentation is a serious impediment. Although ChatGPT may provide sources upon request, when it does provide sources, they must still be verified because ChatGPT may provide nonsensical answers.<sup>18</sup>
4. As a training tool, the current version is sadly lacking: The Federal Financial Institutions Examination Council’s “BSA/AML Examination Manual”<sup>19</sup> remains not only a useful tool but an authoritative source—even if it is wrong, if it is in the manual, your regulatory interlocutors will be hard-pressed to challenge you.
5. Criminals will like ChatGPT’s simplicity and ease of use. They are not known for checking source documents or looking for citations, so there is no impediment there. But that also means they may get it wrong, which is a great help to those of us in the AML/CTF field.
6. Even if all of the above tells you nothing you do not already know, we hope you will agree on one thing: Human intervention will be a necessary part of any effective compliance framework for some time to come. Unlike elevator operators, phone operators, parking lot attendants and other jobs requiring mechanistic responses, evaluating risk factors and red flags; detecting, investigating and analyzing suspicious activity; as well as advising the business line on the risks of doing what they always want to do (onboard, maintain, protect and defend the client) will still be a fundamental part of compliance and require the complex logic, reasoning and intuitive thinking that only humans are capable of, at least for now.
7. Finally, the AI landscape is changing so quickly that everything we have written about it will be outdated eventually, and some of it by the time this article is published. 

*Amanda Bini, legal research consultant, Law Office of Ross Delston*

*Ross Delston, CAMS, independent American attorney and expert witness, Law Office of Ross Delston*

*The authors wish to acknowledge the assistance provided by Dr. Neha Singh, AI/machine learning, natural language processing and data science expert.*

<sup>1</sup> Akash Takyar, “AI Use Cases & Applications Across Major Industries,” *LeewayHertz*, <https://www.leewayhertz.com/ai-use-cases-and-applications/>

<sup>2</sup> “Dark Web Crimes,” *FindLaw*, <https://www.findlaw.com/criminal/criminal-charges/dark-web-crimes.html>

<sup>3</sup> “‘Pig Butchering’ Scams: What They Are and How to Avoid Them,” *FINRA*, December 13, 2022, <https://www.finra.org/investors/insights/pig-butchering-scams>

<sup>4</sup> Miles Brundage, Katie Mayer, Tyna Eloundou, et al., “Lessons learned on language model safety and misuse,” *OpenAI*, March 3, 2022, <https://openai.com/research/language-model-safety-and-misuse>

<sup>5</sup> David Nield, “How ChatGPT and Other LLMs Work—and Where They Could Go Next,” *Wired*, April 30, 2023, <https://www.wired.com/story/how-chatgpt-works-large-language-model/>

<sup>6</sup> Sara Merken, “New York lawyers sanctioned for using fake ChatGPT cases in legal brief,” *Reuters*, June 26, 2023, <https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/>

<sup>7</sup> James Vincent, “OpenAI sued for defamation after ChatGPT fabricates legal accusations against radio host,” *The Verge*, June 9, 2023, <https://www.theverge.com/2023/6/9/23755057/openai-chatgpt-false-information-defamation-lawsuit>

<sup>8</sup> “Introducing ChatGPT,” *OpenAI*, November 30, 2022, <https://openai.com/blog/chatgpt>

<sup>9</sup> This information was obtained directly from ChatGPT. It should be noted that ChatGPT sometimes writes plausible-sounding but incorrect or nonsensical answers. Please view the following source for more information: “Introducing ChatGPT,” *OpenAI*, November 30, 2022, <https://openai.com/blog/chatgpt>

<sup>10</sup> *Ibid.*

<sup>11</sup> *Ibid.*

<sup>12</sup> Jeffrey Dastin, “Amazon scraps secret AI recruiting tool that showed bias against women,” *Reuters*, October 10, 2018, <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>

<sup>13</sup> This information was obtained directly from ChatGPT. It should be noted that ChatGPT sometimes writes plausible-sounding but incorrect or nonsensical answers. Please view the following source for more information: “Introducing ChatGPT,” *OpenAI*, November 30, 2022, <https://openai.com/blog/chatgpt>

<sup>14</sup> *Ibid.*

<sup>15</sup> “Section 314(b) Fact Sheet,” *Financial Crimes Enforcement Network*, December 2020, <https://www.fincen.gov/sites/default/files/shared/314factsheet.pdf>

<sup>16</sup> *Ibid.*

<sup>17</sup> This information was obtained directly from ChatGPT. It should be noted that ChatGPT sometimes writes plausible-sounding but incorrect or nonsensical answers. Please view the following source for more information: “Introducing ChatGPT,” *OpenAI*, November 30, 2022, <https://openai.com/blog/chatgpt>

<sup>18</sup> *Ibid.*

<sup>19</sup> “BSA/AML Examination Manual,” *Federal Financial Institutions Examination Council*, <https://bsaaml.ffiec.gov/manual>

# Let’s talk about your crypto AML program.

ACAMS provides focused training and global insights to help your organization prepare for change in the crypto AML landscape.

Visit our **Crypto Hub** today to discover the right tools for your team: [www.acams.org/crypto](http://www.acams.org/crypto)



**ACAMS** 



# FINCEN'S BENEFICIAL OWNERSHIP:

## CLARITY OR CONFUSION?

As of January 1, 2024, many U.S. companies will be required to report details of their beneficial owners, i.e., individuals who benefit from ownership or control of the company, to the Financial Crimes Enforcement Network (FinCEN).<sup>1</sup> The bureau is now launching an educational outreach program to walk companies through the new reporting rules and offer guidance on how they can stay in compliance while it continues to hash out changes to the customer due diligence (CDD) rule.

Beyond the reporting requirements, access rules and likely changes to the CDD rule, what does this all mean for our anti-money laundering (AML) programs? What information must we consider and where must we consider it in our due diligence programs; or perhaps more importantly, should a lack of information impact the risk rating?

### How we got here

Following a long history of know your customer (KYC) and beneficial ownership regulatory efforts initiated by the Federal Reserve in the 1990s, FinCEN embarked on additional mandates by crafting the proposed CDD rule, which was finalized in 2016. Over the ensuing years, federal officials have repeatedly and publicly articulated the need for the U.S. to enhance and improve authorities' ability to collect beneficial ownership information (BOI).

On September 29, 2022, FinCEN issued its long-awaited BOI reporting rule, the first of three rules in this area required by the Corporate Transparency Act (CTA). This rule laid out the requirements for "reporting companies," as defined in the rule, to provide information about the company's beneficial owners to FinCEN.

Following this, on December 15, 2022, FinCEN issued the second rule required under the CTA: A Notice of Proposed Rulemaking (NPRM),<sup>2</sup> which deals with access to information reported to FinCEN. Now, FinCEN is working on revisions to the CDD rule mandated by the CTA to bring it into alignment with the beneficial ownership rules.

The BOI reporting rule, which was finalized on September 29, 2022, places the onus on a "reporting company" to report BOI to FinCEN along with information regarding the "company applicant," i.e., the person at the reporting company who submits the BOI report.<sup>3</sup> While the BOI reporting rule generally retains the notion of 25% ownership interest, it provides "standards and mechanisms for determining whether an individual owns or controls 25 percent ownership interest in a reporting company"<sup>4</sup> and greatly expands the granularity of the

definition regarding “substantial control.” This information is reported to FinCEN and stored in a FinCEN database, the Beneficial Ownership Secure System (BOSS).

BOI reported to FinCEN is deemed confidential and should not be disclosed except as authorized. The CTA provides specific circumstances under which BOI may be accessed. FinCEN’s NPRM regarding access to BOI, issued on December 15, 2022, enumerates these as follows:

1. Disclosure by FinCEN
  - a. “Disclosure to Federal agencies for use in furtherance of national security, intelligence, or law enforcement activity
  - b. Disclosure to state, local, and tribal law enforcement agencies for use in criminal or civil investigations
  - c. Disclosure for use in furtherance of foreign national security, intelligence, or law enforcement activity
    - i. On behalf of a law enforcement agency, prosecutor, or judge of another country
    - ii. On behalf of a foreign central authority<sup>5</sup> under an applicable international treaty, agreement or convention
  - d. Disclosure “to facilitate compliance with customer due diligence requirements”<sup>6</sup>
    - i. Financial institutions (FIs)
    - ii. Regulatory agencies

When disclosed by FinCEN, BOI can be used solely for the purposes for which it was disclosed. The NPRM includes security and confidentiality requirements for entities to which confidential information is disclosed.

The CTA also requires FinCEN to update the current CDD rule issued in May 2016. The deadline for that update is one year after the January 1, 2024, effective date of the BOI reporting rule. The acting director of FinCEN recently stated that FinCEN is actively “working toward that goal.”<sup>7</sup>

## BOI REPORTED TO FINCEN IS DEEMED CONFIDENTIAL AND SHOULD NOT BE DISCLOSED EXCEPT AS AUTHORIZED

### Today’s CDD rule

The current CDD rule requires FIs, notwithstanding certain exemptions, to identify the beneficial owner as:

- “(1) Each individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer; and
- (2) A single individual with significant responsibility to control, manage, or direct a legal entity customer, including:
  - (i) An executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or
  - (ii) Any other individual who regularly performs similar functions.

(3) If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, the beneficial owner for purposes of paragraph (d)(1) of this section shall mean the trustee. If an entity listed in paragraph (e)(2) of this section owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, no individual need be identified for purposes of paragraph (d)(1) of this section with respect to that entity’s interests.”<sup>8</sup>

### What does all this mean for compliance professionals and their business partners?

Certainly, the period between the effective date of the reporting rule and the reconciliation of the CDD rule to CTA will cause confusion. For instance, how will the provisions of the BOI reporting and access to information reported to FinCEN rules be incorporated into the current CDD rule? And how will the current CDD rule change?

Further, how should a regulated FI incorporate the BOI reporting and access to information reported to FinCEN rules into their AML and CDD efforts? What impact should the reporting of BOI for a reporting company by a company applicant have on the risk rating for that company? Perhaps more importantly, when access to the data reported to FinCEN is requested by an FI, how should the lack of consent by a reporting company be incorporated into the risk rating for that customer?

FIs now need to be thinking about how they will upgrade their policies, procedures and, importantly, their overall and customer risk assessment methodologies to address BOI availability, access and reconciliation.

It is also not a far-fetched idea that regulators might use their ability set forth in 31 CFR 1010.955(b)(4) of the proposed access to information

reported to FinCEN regulation to compare information reported to FinCEN to that acquired by the FI during its risk-based CDD process, requiring the institution to justify each difference. This will call into question processes that may not have been challenged previously, such as the risk-based approach taken by FIs to collect and assess the BOI available to them. It is for this reason that FIs should request access to the BOI from the reporting company. If access is not granted, the risk rating for that customer should minimally increase. Policies should also be set forth outlining when a customer or potential customer should no longer be considered, given the fact that access was not granted.

Finally, while the CTA’s and FinCEN’s final and proposed rules impose strict confidentiality and access requirements regarding BOI, unlike the European Union’s (EU) Fifth AML Directive (5AMLD), the decision by the European Court of Justice to limit unfettered public access to BOI will undoubtedly have a dampening effect on CDD and the inclusion of BOI in that process. Global FIs, including those based in the EU, will need to closely monitor events in this area. **AT**

**Stephen D. Marshall, director, FinScan Advisory Services, Pittsburgh, PA, USA, [Smarshall@innovativesystems.com](mailto:Smarshall@innovativesystems.com)**

<sup>1</sup> “Beneficial Ownership Information Reporting,” *Financial Crimes Enforcement Network*, <https://www.fincen.gov/boi>

<sup>2</sup> “FinCEN Issues Notice of Proposed Rulemaking Regarding Access to Beneficial Ownership Information and Related Safeguards,” *Financial Crimes Enforcement Network*, December 15, 2022, <https://www.fincen.gov/news/news-releases/fincen-issues-notice-proposed-rulemaking-regarding-access-beneficial-ownership>

<sup>3</sup> Under the CTA there are 23 exemptions to the reporting requirements. These are enumerated specifically in the BOI reporting rule.

<sup>4</sup> “Beneficial Ownership Information Reporting Rule Fact Sheet,” *Financial Crimes Enforcement Network*, September 29, 2022, <https://www.fincen.gov/beneficial-ownership-information-reporting-rule-fact-sheet>

<sup>5</sup> “Beneficial Ownership Information Access and Safeguards, and Use of FinCEN Identifiers for Entities,” *Federal Register*, December 16, 2022, <https://www.federalregister.gov/documents/2022/12/16/2022-27031/beneficial-ownership-information-access-and-safeguards-and-use-of-fincen-identifiers-for-entities>

<sup>6</sup> *Ibid.*

<sup>7</sup> “Prepared Remarks of FinCEN Acting Director Himamauli Das During the ABA/ABA Financial Crimes Enforcement Conference,” *Financial Crimes Enforcement Network*, December 6, 2022, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-himamauli-das-during-abaaba-financial-crimes>

<sup>8</sup> “Customer Due Diligence Requirements for Financial Institutions,” *Federal Register*, May 11, 2016, <https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions>

# FARNOUSH MIRMOEINI: LEVERAGING TECHNOLOGY



**A** CAMS Today Europe Digital sat down with Farnoush Mirmoeini, the founder of KYC Hub and the recipient of the U.K.'s Techwomen100 award in 2022. She was also listed on Innovate Finance's Women in FinTech Powerlist in 2022. With over 13 years of experience working with financial technology (fintech) and banking, Mirmoeini has dedicated her career to improving the financial landscape using technology. Following the start of her career as a financial engineer for QulC Financial Technologies, Mirmoeini worked as a quantitative analyst at HSBC and was a co-founder of Obsessory.

Since earning her Bachelor of Applied Science degree in electrical engineering from the University of British Columbia, Mirmoeini has earned her Master of Business Administration degree in exchange from the London Business School, a Master of Business Administration degree in finance and entrepreneurship from the University of Michigan

and a Master of Applied Science degree in engineering from the University of British Columbia.

**ACAMS Today Europe Digital (AT Europe):** Tell us what inspired you to create KYC Hub and what are some of the key achievements your company has executed?

**Farnoush Mirmoeini (FM):** I believe that quality anti-money laundering (AML) compliance solutions are the backbone of our global economy. I have seen so many huge economic fallouts that could have been avoided by having a robust due diligence system that it felt almost like a moral duty to act on it. As the world learns to exploit technology for all industries, financial crime also uses those same tools to increase sophistication. Seeing these challenges businesses faced with regulatory compliance led to the creation of KYC Hub.<sup>1</sup> Our focus on intelligent automation and a risk-driven approach has proven to be instrumental in reshaping compliance efforts.

## TO STAY AHEAD OF FINANCIAL CRIMES IN THE EVER- EVOLVING FINTECH LANDSCAPE, PROFESSIONALS NEED TO ADOPT A PROACTIVE APPROACH OR LOSE THE BATTLE

**AT Europe:** Machine learning relies heavily on quality data. How can financial institutions (FIs) leverage this tool with limited human expertise in this area?

**FM:** Humans are good at acquiring great depth in knowledge, but with limited time, we might lose out on breadth. This is where technology, like machine learning with continuous learning, comes in. Firms should use a combination of vendors and in-house development in order to achieve the best benefit from artificial intelligence (AI)/machine

learning technologies. Also, it is important to invest in building advanced data pipelines and proper training datasets before attempting to use AI models.

**AT Europe:** As technology quickly evolves, how can professionals in the fintech industry stay ahead of financial crimes?

**FM:** In the age of technology, the uphill battle that the industry faces with financial crime is no different than an arms race. To stay ahead of financial crimes in the ever-evolving fintech landscape, professionals need to adopt a proactive approach or lose the battle. Continuous learning and keeping up with trends in financial crime prevention are required for this. Engaging with industry forums, attending conferences and networking with peers can provide valuable insights. In addition, leveraging advanced technologies like AI and machine learning can provide a competitive edge in identifying and mitigating financial risks.

**AT Europe:** You believe that it is better to be agile rather than plan. Can you share an anecdote where you had success applying this viewpoint?

**FM:** Entrepreneurs should embody the industry from which they come. Working in an industry as fast-paced and dynamic as financial technology, one must understand that agility must take precedence over rigidity. One memorable instance I can recall was an issue with a product on the eve of an important proposal. We faced unexpected technical challenges that threatened our timeline. This is to be expected. Not all plans will be executed with 100% accuracy and hoping for that is a bad strategy. Instead of strictly keeping to the initial plan, we promptly pivoted our approach, allocating resources where they were needed most. It confirmed my conviction that flexibility frequently trumps rigid adherence to pre-established plans in the fast-paced world of technology.

**AT Europe:** Why is it important for you to promote the younger generation of women?

**FM:** Promoting the younger generation of women is something that should be a part of any entrepreneur's journey. I know firsthand the power of mentorship and paving the way for future leaders. As a female founder in the fintech industry, I've experienced firsthand the importance of representation and support in a traditionally male-dominated sector. It is a fact that the experiences of women in any sector are vastly different from those of men.

We should always work to raise the new generation. By actively advocating for and empowering young women, we can create a more inclusive and diverse tech community. This not only benefits individual careers but also contributes to a more innovative and dynamic industry as a whole. [AT](#)

Interviewed by: ACAMS Today Europe Digital staff, ACAMS, editor@acams.org

<sup>1</sup> KYC Hub homepage, <https://www.kychub.com/>

# Birth of a global watchdog:

## *The Egmont Group*

In stark contrast to the cold day of June 9, 1995, the atmosphere at the Egmont-Arenberg Palace in Brussels was ablaze with tension and anticipation. As members of the Belgian financial intelligence unit (FIU), the Cellule de Traitement des Informations Financières (CTIF-CFI) patiently awaited the arrival of the train that held 100 representatives from 24 nations and eight international bodies from the Financial Action Task Force's (FATF) plenary meeting in The Hague; they felt that they were venturing into uncharted territory.<sup>1</sup>

One thing was certain: Cross-border cooperation among “disclosure receiving agencies” or “financial information units” could not continue blindly.<sup>2</sup> Many within the FIU circles knew that sharing information among the various units could benefit law enforcement (LE) worldwide and enhance mutual efforts in the fight against money laundering. There was a need for an organization of united entities.<sup>3</sup>

Little did they know that they were about to make history.

## Lacking cohesion

The Egmont Group was not a mere milestone but the development of six years of international anti-money laundering (AML) achievements, beginning with the Vienna Convention of 1988. Organized by the United Nations (U.N.) to tackle the problem of drug trafficking, the Convention called for the creation of mechanisms to facilitate partnerships in money laundering investigations.

The idea gained additional momentum when, in early 1990, FATF released its 40 Recommendations.<sup>4</sup> In particular, Recommendation 24 urged countries to consider the “feasibility and utility” of national central agencies to be used by financial institutions to report domestic and international transactions above a certain threshold.<sup>5</sup>

FIUs began to timidly emerge in the early '90s, particularly in Europe, with the mention of the need to create such units in the first Commission Report on the implementation of the European Union AML Directive of 1990.<sup>6</sup>

Yet, the vagueness and lack of guidelines for their establishment birthed agencies with disparate forms and ways of functioning. Goodwill and memorandums of understanding (MOUs) were often the basis for transnational partnerships among these units, but international laws and the diversities of such organizations often posed obstacles to effective communication.<sup>7</sup>

Stanley E. Morris, then director of the U.S. Financial Crimes Enforcement Network (FinCEN), knew that the success of his agency and other FIUs depended on their synergies. FinCEN needed allies and he found like-mindedness in a nation the size of Maryland.

## The search for allies

In his years as deputy director of the White House Drug Office in the late '80s and early '90s, Morris understood that the way to have an impact on the War on Drugs was to block the flow of income of criminal organizations. “Supply of drugs was up, prices down and there had been no reduction in use,” Morris recalls. “So, I looked at what might actually make a difference if you could not stop the supply or the usage.... It was to go after the profits.”<sup>8</sup>

Not many within the U.S. government shared his vision. When Morris became FinCEN's second director in 1994, he was able to pass stronger AML laws, but roadblocks kept the agency from achieving its full potential as an FIU.<sup>9</sup>

“As a bureaucrat, I knew FinCEN was never going to get the attention or the funding of the ‘big’ agencies ... neither the financial regulatory agencies nor the numerous federal law enforcement agencies.”<sup>10</sup>

International borders and the period's challenging communication were also a constraint to obtaining intelligence on inter-country financial movements. Morris knew that what FinCEN needed was allies. “So, where could we find those allies and the best place to look was at the margins of the Financial Action Task Force and the Council of Europe's money laundering group.”<sup>11</sup>

As head of the U.S. delegation to FATF, Morris approached Dr. Jean Spreutels, then head of the Belgian delegation and director of the CTIF-CFI, during a FATF plenary meeting in the Netherlands. “I knew that he had been active in organizing national drug enforcement units in the past and I think he was following the same route I was, which was moving from drug interdiction to drug profit interdiction.”<sup>12</sup>

The result was the signing of an MOU between the two FIUs on July 8, 1994—an agreement that still stands today. “Our negotiations of July 1994 clearly revealed the difficulty of setting up a cooperative relationship between units, where legal differences often prevented dialogue in spite of having core missions,” Spreutels recalls in his Egmont Group's 10th-anniversary address. “We had overcome this obstacle. Yet, shouldn't we try to broaden the basis for cooperation by creating a forum for all anti-money laundering units?”<sup>13</sup>

## An informal meeting

As director of the U.S. Marshals Service throughout most of the '80s, Morris understood that informal contacts were the most efficient way to communicate with potential partners. “The opportunity to attend sessions with other police heads around the world at Interpol conferences where we could exchange contacts permitted a much easier free and quick exchange of information,” he recalls. “I was looking for something similar when Jean and I organized the first Egmont Group meeting.”<sup>14</sup>

Since Brussels was near to where the FATF meetings took place, Spreutels decided to host the gathering in the Belgian capital as he had enough authority to call an international conference without involving the Belgian foreign ministry. The palatial 16th-century Egmont-Arenberg Palace was chosen as the meeting ground.<sup>15</sup>

The two major objectives of the forum were to strengthen global collaboration and pinpoint challenges and solutions related to information exchange. It was also a way to ensure consistency among FIUs and assist the newer and emerging agencies in their development.<sup>16</sup>



“We barely knew the participants,” Boudewijn Verhelst, deputy director of CTIF-CFI remembers, “only that they were performing what we thought to be a similar function.”<sup>17</sup>

On June 9, 1995, representatives of the following FIUs convened in Brussels: The Australian Transaction Reports and Analysis Centre (AUSTRAC), Monaco’s Service d’Information et de Contrôle sur les Circuits Financiers (SICCFIN), the Austrian Financial Intelligence Unit (A-FIU), Spain’s Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC), Belgium’s CTIF-CFI, the U.K.’s Serious Organised Crime Agency (SOCA), the U.S.’s FinCEN, Slovenia’s Office for Money Laundering Prevention (OMLP), Luxembourg’s Cellule de Renseignement Financier (CRF), Sweden’s Finanspolisen Rikskriminalpolisen (FIPO), FIU Netherlands, France’s Intelligence Processing and Action Against Illicit Financial Networks Unit (TRACFIN) and Norway’s Financial Intelligence Unit (ØKOKRIM). Additional nations without an established FIU were also in attendance and included Canada, the Czech Republic, Finland, Germany, Greece, Iceland, Italy, Japan, New Zealand, Portugal and Switzerland.<sup>18</sup>

While many embraced the idea of an informal forum, certain attendees were not convinced. Many saw the group as “another travel agency,” pointing out that Interpol channels already existed for the exchange of information. One participant was even astounded by the concept of an administrative unit situated within an LE context.<sup>19</sup>

To entice the representatives to take part in the meeting, FinCEN gave an incentive. “The old agencies were stuck with buildings full of old-style main frame computers with large discs and large staffs to man them,” Morris recalls. “So, I proposed for



those units that wanted [it], we would create a communication system that would be secure and separate from the mainframe computer world that most governments were operating within. This, of course, gave the FIUs something that made them special, and I believe helped press governments to establish the laws and regulations necessary to support anti-money laundering initiatives.”<sup>20</sup>

### Aftermath

The outcome of the meeting was successful, with numerous FIUs showing interest and enthusiasm in continuing the informal meetings.

The pivotal outcome of the gathering was the formation of three working groups tasked with research, analysis and technical assistance, among other endeavors: The Legal Working Group, the Technology Working Group and the Analytical Tools/ Training Working Group.<sup>21</sup>

These working groups, particularly the legal ones, would become important in AML. Through questionnaires distributed among the members and an analysis of their answers, they were able to draft the first official international definition of an FIU, which was approved by the group during their 1996 conference.

The definition would later be amended in 2004 due to the evolution of terrorism.<sup>22</sup>

This early work of the group was later picked up by the U.N., which included the definition of an FIU in the United Nations’ Palermo Convention.<sup>23</sup>

The Egmont Group’s first meeting also benefited its members. When reminiscing on the communication system that was set up by FinCEN, Morris believes that it gave them “bragging” rights with other U.S. agencies. “You have a case in Slovenia or Panama and want information quickly... FinCEN could provide that and often the information exchanged was not subject to Bank Secrecy or other protections,” he states. “Egmont was a very helpful tool for FinCEN in the bureaucratic wars for attention, laws and funding. I suspect that other FIUs were able to use it as well.”<sup>24</sup>

### The evolution of a revolution

As the gatherings continued, the Egmont Group evolved into one of the most influential organizations in AML.

The work of the group and the expansion of FIUs worldwide was reflected in the 1998 20th Special

Session of the U.N. General Assembly on the problem of drugs, which recognized that the fight against money laundering can be won “only through international cooperation and the establishment of bilateral and multilateral information networks such as the Egmont Group.”<sup>25</sup>

“In less than 10 years, an idea that was new and largely unknown had become the international standard,” Morris recalls. “Without Egmont, that would not have occurred.”<sup>26</sup>

As the working groups expanded over the years, CTIF-CFI and FinCEN agreed to establish in 2002 a coordination body named the Egmont Committee. The working groups continue to develop, cooperate and share expertise as per the group’s mission.<sup>27</sup> There are currently six working groups.

In 2007, the Egmont Group Charter was signed in Bermuda, changing the informal status of the association to a structured organization with a constitutional base and a permanent secretariat.<sup>28</sup>

Its members also grew exponentially, currently encompassing 171 FIUs from around the globe.<sup>29</sup> The expanding growth of FIUs is also due to the group’s work throughout the years.

### Headless but united

When looking back at the struggle to find a proper name for the organization, Morris recalls a humorous anecdote from Spreutels. Following the 1995 meeting, Morris thought that the name he had come up with—Egmont Group—had little significance outside of the first meeting grounds.<sup>30</sup>

“Jean and I never took ourselves too seriously and he always had a kind of a mischief look in his eye and a wonderful sense of humor,” he states. “So, Jean disagreed. You see, Stan, the Egmont Group is a perfect name. The Duke of Egmont became an irritant to the Spanish King Philip II and the king had the duke beheaded. Perfect. The Egmont Group does not have a head either, said Jean. It only has colleagues committed to a common goal.”<sup>31</sup> **AT**

Stefano Siggia, CAMS, senior consultant, Pideeco, Belgium, stefano@pideeco.be, [in](#)

<sup>1</sup> “Annual Report June 2009–July 2010,” *Egmont Group*, p. 2, 2010.

<sup>2</sup> Ibid.

<sup>3</sup> “Annual Report 2014–2015,” *Egmont Group*, p. 4, 2015, [https://egmontgroup.org/wp-content/uploads/2021/09/Egmont\\_Group\\_Annual\\_Report\\_2014-2015.pdf](https://egmontgroup.org/wp-content/uploads/2021/09/Egmont_Group_Annual_Report_2014-2015.pdf)

<sup>4</sup> “Annual Report June 2009–July 2010,” *Egmont Group*, p. 5, 2010.

<sup>5</sup> “The Forty Recommendations of the Financial Action Task Force on Money Laundering,” *Financial Action Task Force*, 1990, <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%201990.pdf>

<sup>6</sup> Valsamis Mitsilegas, “New Forms of Transnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights Part 2,” *Journal of Money Laundering Control* Vol. 3 No.3, p. 250, January 1, 2000.

<sup>7</sup> JF Thony, “Processing Financial Information in Money Laundering Matters: The Financial Intelligence Units,” *European Journal of Crime, Criminal Law, and Criminal Justice* Vol. 4, pp. 264–279, 1996.

<sup>8</sup> Personal interview with Stanley E. Morris conducted on July 20, 2023.

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

<sup>11</sup> Ibid.

<sup>12</sup> Ibid.

<sup>13</sup> “Annual Report 2014–2015,” *Egmont Group*, p. 5, 2015, [https://egmontgroup.org/wp-content/uploads/2021/09/Egmont\\_Group\\_Annual\\_Report\\_2014-2015.pdf](https://egmontgroup.org/wp-content/uploads/2021/09/Egmont_Group_Annual_Report_2014-2015.pdf)

<sup>14</sup> Personal interview with Stanley E. Morris conducted on July 25, 2023.

<sup>15</sup> Personal interview with Stanley E. Morris conducted on July 20, 2023.

<sup>16</sup> “Annual Report 2014–2015,” *Egmont Group*, p. 4, 2015, [https://egmontgroup.org/wp-content/uploads/2021/09/Egmont\\_Group\\_Annual\\_Report\\_2014-2015.pdf](https://egmontgroup.org/wp-content/uploads/2021/09/Egmont_Group_Annual_Report_2014-2015.pdf)

<sup>17</sup> “Annual Report June 2009–July 2010,” *Egmont Group*, p. 2, 2010.

<sup>18</sup> Ibid. p. 5.

<sup>19</sup> Ibid. p. 2.

<sup>20</sup> Personal interview with Stanley E. Morris conducted on July 20, 2023.

<sup>21</sup> “Annual Report 2014–2015,” *Egmont Group*, p. 5, 2015, [https://egmontgroup.org/wp-content/uploads/2021/09/Egmont\\_Group\\_Annual\\_Report\\_2014-2015.pdf](https://egmontgroup.org/wp-content/uploads/2021/09/Egmont_Group_Annual_Report_2014-2015.pdf)

<sup>22</sup> Wouter H. Muller et al., *Anti-money Laundering: International Law and Practice*, Wiley, pp. 7–8, 2007.

<sup>23</sup> Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*, *World Bank Publications*, pp. VII–3, 2006.

<sup>24</sup> Personal interview with Stanley E. Morris conducted on July 20, 2023.

<sup>25</sup> Valsamis Mitsilegas, “New Forms of Transnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights Part 1,” *Journal of Money Laundering Control* Vol. 3 No.2, p. 157, April 1, 1999.

<sup>26</sup> Personal interview with Stanley E. Morris conducted on July 20, 2023.

<sup>27</sup> “Annual Report June 2009–July 2010,” *Egmont Group*, p. 5, 2010.

<sup>28</sup> “Annual Report 2014–2015,” *Egmont Group*, p. 7, 2015, [https://egmontgroup.org/wp-content/uploads/2021/09/Egmont\\_Group\\_Annual\\_Report\\_2014-2015.pdf](https://egmontgroup.org/wp-content/uploads/2021/09/Egmont_Group_Annual_Report_2014-2015.pdf)

<sup>29</sup> “About the Egmont Group,” *Egmont Group*, <https://egmontgroup.org/about/>

<sup>30</sup> Personal interview with Stanley E. Morris conducted on July 20, 2023.

<sup>31</sup> Ibid.



# EU's approach to sanctions

Companies involved in transnational business are concerned about sanctions primarily because of the U.S. Office of Foreign Assets Control (OFAC), which is highly active in terms of enforcement and imposes large penalties on sanctions violators. Conversely, while the European Union (EU) has also been active in imposing sanctions, it has not been as effective regarding sanctions enforcement. However, the latest developments in Brussels suggest that this might be about to change.

## Sanctions enforcement: EU vs. U.S.

Sanctions have long been a powerful tool in the arsenal of international diplomacy. The EU and the U.S. have utilized sanctions to pressure nations and entities that violate international norms. However, while the objectives might be similar, these two entities' enforcement mechanisms and challenges differ significantly.

The U.S., with its robust financial system and global influence, has been at the forefront of implementing and enforcing sanctions. OFAC administers and enforces economic and trade sanctions. The U.S. employs a comprehensive approach, targeting individuals, entities and even entire sectors, such as energy or finance. For instance, the U.S.

sanctions against Iran have been particularly stringent, targeting its oil exports and financial institutions.

More importantly, when it comes to enforcement, OFAC is an institution that internationally operating companies need to take seriously. The numbers speak for themselves. In the first nine months of 2023 alone, OFAC has imposed civil penalties on sanctions violators amounting to \$567 million, targeting companies such as Swedbank, British American Tobacco, Microsoft and Wells Fargo Bank.<sup>1</sup>

On the other hand, the EU's approach to sanctions has been more nuanced. Historically, the EU has been using sanctions as a foreign policy instrument, but countering violations has always posed challenges.<sup>2</sup> The bloc's sanctions are often designed to be less disruptive, focusing on targeted measures like asset freezes or travel bans. However, as mentioned in a *Global Investigations Review* piece, "The use of trade and financial sanctions by the European Union has become an increasingly important element of the bloc's foreign policy."<sup>3</sup> In reaction to Russia's invasion of Ukraine, the EU has swiftly built one of the most comprehensive and robust sanctions regimes ever seen.<sup>4</sup>

Nevertheless, due to the inherent weaknesses of the EU's sanctions regime, the enforcement has been lagging, making the EU seem less of

a threat to companies with potential sanctions exposure. Not only have there been no major U.S.-styled penalties against sanctions violators to speak of, but there is also no EU-wide platform on which to find such cases, leading to a lack of legal clarity with regard to what may constitute an "effective, proportionate and dissuasive" penalty.<sup>5</sup>

## Weaknesses in the EU's sanctions regime

The EU's sanctions regime has faced criticism for its perceived lack of uniformity and strictness. One of the primary challenges is the need for a consensus among member states, which can lead to delays or watered-down measures. In addition, the EU's complex bureaucratic structure can sometimes hinder swift action.

Most importantly, however, the EU has faced serious challenges in countering violations of its sanctions. The main challenge is the fact that "the day-to-day administration and enforcement of sanctions is delegated to the competent authorities of each [member state] within the EU."<sup>6</sup> In addition, "Each [member state] must determine, therefore, the penalties that it considers to be sufficiently robust to deter transgressions, and draft and issue guidance designed to provide clarity for natural and legal persons as to their sanctions compliance obligations."<sup>7</sup>



This lack of consistency presents a serious challenge. While some member states have specific departments dedicated to investigating breaches of EU sanctions, other member states appear to be laxer in this regard. The reason for this could be as simple as a lack of a competent and properly trained workforce or even a lack of political will to pursue stringent enforcement. Furthermore, some member states might favor protecting the economic interests of important domestic companies, which could be negatively impacted by stricter sanctions enforcement.<sup>8</sup>

Compounding the issue is the lack of uniformity with regard to the penalties for sanctions violations across the EU. According to the aforementioned *Global Investigations Review* article, “The EU’s 27 separate judicial systems each apply individual definitions and approaches, in particular when it comes to the question of whether a sanctions violation can be considered as a criminal and/or administrative offence.”<sup>9</sup>

In 12 member states, the violation of sanctions is solely a criminal offense. “For 13 member states, the violation of sanctions can be considered either an administrative or criminal offence.”<sup>10</sup> The remaining two member states currently enforce the violation of sanctions exclusively by means of administrative penalties.<sup>11</sup>

The apparent weakness in the EU’s sanctions enforcement regime has been exposed in several recent media investigations in EU countries.

For example, in May 2023, the Russian Anti-Corruption Foundation published an investigation on the family of Boris Obnosov, the head of Russia’s Tactical Missiles Corporation, an entity sanctioned by the EU since June 2022. “The report found his family members to own a four-story house worth six million euros, a penthouse worth over one million euros, and several other properties in Prague.”<sup>12</sup>

The properties were, according to the Czech media, eventually frozen in August 2023 after the Czech Ministry of Foreign

Affairs placed Obnosov and his family members on the Czech sanctions list.<sup>13</sup> The Czech Republic thus acted unilaterally, as placing Obnosov on an EU sanctions list would require a unanimous agreement of the 27 member states, which would likely take much longer if it even ever materialized.

In June 2023, German media reported that despite being sanctioned by the EU, the Russian propaganda channel Ruptly GmbH, fully owned by the sanctioned Moscow-based media company TV-Novosti, continued to produce video content from Berlin. TV-Novosti was placed on the EU’s sanctions list in December 2022.<sup>14</sup>

According to a media report from August 2023, Ruptly GmbH seems to have transferred its assets to another German-based company named Lensem GmbH, fully owned by an Armenian entity named Roxxon. However, the media report provides evidence that the new company simply took over Ruptly’s employees and carried on with the same activity. The German authorities refused to provide comments to the media on this case.<sup>15</sup>



### Shifting the focus to enforcement

In December 2022, the EU appointed a special sanctions envoy, David O’Sullivan, after several EU countries reportedly “pushed the European Commission to change its focus from adopting new sanctions against Russia to enforcing the existing ones.”<sup>16</sup> O’Sullivan’s role is to “ensure continuous, high-level discussions with third countries to avoid the evasion or even the circumvention” of Russia-related sanctions.<sup>17</sup>

In July 2023, EU members of parliament in the Civil Liberties Committee adopted a draft negotiating mandate for a new EU law on violating and circumventing EU sanctions. “It would introduce a common definition of violations and minimum penalties to ensure that they are punished as criminal offences everywhere in the EU”<sup>18</sup> with common definitions and dissuasive penalties.

The European Parliament states, “According to the proposal, violating and circumventing the sanctions should be punishable criminal offences carrying prison sentences of a maximum of five years and fines of up to ten million euro.... In the adopted text, [members of the European

Parliament (MEPs)] set the maximum fine that companies would pay to 15% of overall annual turnover and added new aggravating circumstances, for example, war crimes and obstructing investigations, that lead to higher penalties.”<sup>19</sup>

The European Parliament also adds that circumventing would also “be punishable and would include practises such as concealing or transferring funds that should be frozen, hiding the true ownership of property, and not reporting sufficient information.”<sup>20</sup>

The next step is for EU MEPs to start inter-institutional negotiations with EU governments to decide the final phase of the legislation.<sup>21</sup> However, it needs the backing of all member states, which have traditionally been cautious about reforms that require change to their criminal laws.

Furthermore, earlier in 2023, the Netherlands put forward a proposal, supported by several EU countries, to establish a centralized EU sanctions watchdog to tackle mass circumvention of EU sanctions centrally from Brussels. The proposal includes measures to strengthen the feedback loop between enforcement practice at the national level and the EU level.

Moreover, if the above-mentioned EU law on the unification of sanctions enforcement gets passed, a centralized EU sanctions watchdog could send cases directly to the EU’s general prosecutor.<sup>22</sup>

These developments highlight a potential transformation in the EU’s sanctions enforcement strategy, aiming for a more robust and coordinated approach that aligns with the proactive and forceful stance taken by the U.S. Nevertheless, to create a more centralized sanctions enforcement mechanism, every European capital will need to be first convinced to relinquish a certain dimension of their national sovereignty, not exactly a simple task in today’s Europe. **AT**

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

<sup>1</sup> Civil Penalties and Enforcement Information, *Office of Foreign Assets Control*, <https://ofac.treasury.gov/civil-penalties-and-enforcement-information>

<sup>2</sup> Dr. Kim B. Olsen and Simon FASTERKJÆR KJELDSSEN, “Strict and Uniform: Improving EU Sanctions Enforcement,” *DGAP*, September 29, 2022, <https://dgap.org/en/research/publications/strict-and-uniform-improving-eu-sanctions-enforcement>

<sup>3</sup> David Savage, “EU Sanctions Enforcement,” *Global Investigations Review*, July 8, 2022, <https://globalinvestigationsreview.com/guide/the-guide-sanctions/third-edition/article/eu-sanctions-enforcement>

<sup>4</sup> Dr. Kim B. Olsen and Simon FASTERKJÆR KJELDSSEN, “Strict and Uniform: Improving EU Sanctions Enforcement,” *DGAP*, September 29, 2022, <https://dgap.org/en/research/publications/strict-and-uniform-improving-eu-sanctions-enforcement>

<sup>5</sup> Stéphane Bonifassi and Julie Bastien, “EU Sanctions Enforcement,” *Global Investigations Review*, September 29, 2023, <https://globalinvestigationsreview.com/guide/the-guide-sanctions/fourth-edition/article/eu-sanctions-enforcement>

<sup>6</sup> “Sanctions Guidelines—update,” *Council of the European Union*, May 4, 2018, <https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf>

<sup>7</sup> David Savage, “EU Sanctions Enforcement,” *Global Investigations Review*, July 8, 2022, <https://globalinvestigationsreview.com/guide/the-guide-sanctions/third-edition/article/eu-sanctions-enforcement>

<sup>8</sup> Ibid.

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

<sup>11</sup> Dr. Kim B. Olsen and Simon FASTERKJÆR KJELDSSEN, “Strict and Uniform: Improving EU Sanctions Enforcement,” *DGAP*, September 29, 2022, <https://dgap.org/en/research/publications/strict-and-uniform-improving-eu-sanctions-enforcement>

<sup>12</sup> “Team Navalny finds luxury real estate in Czech Republic belonging to family of Russian Tactical Missiles Corporation CEO,” *Meduza*, May 10, 2023, <https://meduza.io/en/news/2023/05/10/team-navalny-finds-luxury-real-estate-in-czech-republic-belonging-to-family-of-russian-tactical-missiles-corporation-ceo>; Alexey Navalny, “The Foreign Life of Russia’s Leading Missile Maker,” *YouTube*, May 10, 2023, <https://www.youtube.com/watch?v=HRzNOBUBYfc>

<sup>13</sup> Katerina Gruntová, “The Czech Republic has put a Russian arms manufacturer, his daughter and son-in-law, who own real estate in Prague, to the sanctions list,” *iROZHLAS*, August 16, 2023, [https://www.irozhlas.cz/zpravy-domov/sankcni-seznam-rusko-cesko-boris-obnosov-rostislav-zorikov\\_2308161550\\_gut](https://www.irozhlas.cz/zpravy-domov/sankcni-seznam-rusko-cesko-boris-obnosov-rostislav-zorikov_2308161550_gut)

<sup>14</sup> “Russian state media continues to produce in Berlin,” *ntv*, June 29, 2023, <https://www.n-tv.de/politik/Russisches-Staatsmedium-produziert-weiter-in-Berlin?article=42425895.html>

<sup>15</sup> Christoph M. Kluge and Claudia von Salzen, “Front company in Berlin?: How a Russian state media could circumvent the sanctions,” *Tagesspiegel*, August 29, 2023, <https://www.tagesspiegel.de/politik/tarnfirma-in-berlin-wie-ein-russisches-staatsmedium-die-sanktionen-umgehen-konnte-10382020.html>

<sup>16</sup> Jakob Hanke Vela and Barbara Moens, “EU’s new sanctions envoy shifts focus to enforcement,” *Politico*, March 1, 2023, <https://www.politico.eu/article/eus-new-sanctions-envoy-set-to-fight-sanction-circumvention/>

<sup>17</sup> “EU appoints David O’Sullivan as International Special Envoy for the Implementation of EU Sanctions,” *European Commission*, December 13, 2022, [https://ireland.representation.ec.europa.eu/news-and-events/news/eu-appoints-david-osullivan-international-special-envoy-implementation-eu-sanctions-2022-12-13\\_en](https://ireland.representation.ec.europa.eu/news-and-events/news/eu-appoints-david-osullivan-international-special-envoy-implementation-eu-sanctions-2022-12-13_en)

<sup>18</sup> Tamer A. Soliman, Jason Hungerford, Paulette Vander Schueren, et al., “Sanctions Weekly Update—Ukraine/Russia Conflict—July 3, 2023,” *Mayer Brown*, July 3, 2023, <https://www.mayerbrown.com/en/perspectives-events/publications/2023/07/sanctions-weekly-update-ukraine-russia-conflict--july-3-2023>

<sup>19</sup> “EU sanctions: new law to crack down on violations,” *European Parliament*, July 6, 2023, <https://www.europarl.europa.eu/news/en/press-room/20230703IPR01909/eu-sanctions-new-law-to-crack-down-on-violations>

<sup>20</sup> Ibid.

<sup>21</sup> Ibid.

<sup>22</sup> Alexandra Brzozowski, “Netherlands calls for EU sanctions enforcement headquarters,” *EURACTIV*, February 20, 2023, <https://www.euractiv.com/section/global-europe/news/netherlands-calls-for-eu-sanctions-enforcement-headquarters/>

# Stopping cross-border illicit financial flows



GRACE JACKSON



MAKSYM MARKEVYCH

**A** CAMS Today Europe Digital spoke to Grace Jackson and Maksym Markevych, who work for the Financial Integrity Group in the Legal Department of the International Monetary Fund (IMF), about their partnership with Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden in a first-of-its-kind technical assistance project to strengthen the effectiveness of anti-money laundering/counter-terrorist financing (AML/CTF) frameworks.

Governors of the Nordic-Baltic central banks reached out to the IMF requesting technical assistance following the money laundering banking scandals from ABLV, Danske Bank, Nordea and Swedbank, involving cross-border payments by nonresidents that exposed financial integrity risks in the financial sector of the region, attracting international scrutiny on the level of nonresident money laundering/terrorist financing risks and highlighting the vulnerabilities related to AML/CTF risk-based supervision of banks in the region.

Jackson is currently working on AML/CTF and proliferation-related issues in the context of IMF-supported programs

and surveillance, as well as capacity development. Over the past few years, she has been heavily involved in fintech-related work (including crypto-assets). More recently, she has been exploring the nexus between financial integrity failures and financial stability.

Markevych works on AML/CTF and other financial integrity and governance topics, primarily for programs supported by IMF, as well as capacity development and surveillance. He focuses on financial sector issues and money laundering/terrorist financing, particularly from cross-border financial flows.

**ACAMS Today Europe Digital (AT Europe):** *The “Nordic-Baltic Regional Technical Assistance Project—Financial Flows Analysis, AML/CTF Supervision, and Financial Stability”<sup>1</sup> report leveraged data analysis to understand money laundering/terrorist financing threats and vulnerabilities. What were some of the key findings?*

**Maksym Markevych (MM):** We see significant value in the analysis of payments data to assess countries’ exposure to money laundering/terrorist

financing risks and detect illicit financial flows. As part of the project with the Nordic-Baltic countries, we applied an unsupervised machine learning algorithm to detect unusual and potentially suspicious patterns of financial flows in the region and discussed with authorities the application of advanced data analytics techniques for AML purposes. Considering that the region has immaterial flows with the countries on the Financial Action Task Force (FATF) and European Commission higher risk lists, the Nordic-Baltic countries can further develop their understanding of higher money laundering/terrorist financing risk countries by incorporating country-specific risk factors and focusing on the counterparty countries with the most material financial flows. In this respect, we analyzed the increasing flows in the region with various financial centers and associated cross-border tax evasion risks. Our analysis also found that understanding cross-border and nonresident exposures of banks can assist in predicting contagion effects from financial integrity breaches and the identification of banks that are the most exposed to money laundering threats to financial stability.



**Grace Jackson (GJ):** On AML/CTF risk-based supervision, a robust money laundering/terrorist financing risk assessment that underpins your supervisory approach remains key. In our work with the eight countries, we could see that there has been a clear investment in supervisor money laundering/terrorist financing risk models, but some gaps remain, notably in advanced data collection and analysis. Having a robust methodology is only one aspect and if there is a lack of accurate and comprehensive data, the output becomes compromised. Two takeaways are the need for more granular data collection (particularly on cross-border payments) and the exploration of supervisory technology (suptech) tools to avoid diverting resources away from other critical supervisory activities. We've captured our findings in an IMF blog post<sup>2</sup> and invite everyone to give it a read.

**AT Europe:** *What recommendation has the IMF presented to Nordic-Baltic central banks to solve cross-border illicit financial flows?*

**GJ:** I'm not sure we'll ever get to a place where countries can "solve" cross-border illicit financial flows. Instead, it's about being realistic and further refining AML/CTF toolkits to prevent (to the best of our ability) and detect these activities, along with having a framework in place that positions country authorities and gatekeepers (including banks) to be one step ahead of criminals trying to exploit the financial system. Moreover, countries really need to think beyond prevention and detection and start quantifying the financial stability impact of money laundering shocks in order to be prepared should these happen. Our analysis shows that banks facing financial integrity issues were looking at a sharp decline in their stock prices and an increase in the perceived credit risk. In addition, spillover effects were significant for other key regional banks, pointing to contagion effects between the affected banks and similar banks.

Overall, this is an understudied area and further collaboration between AML/CTF supervisors, prudential supervisors and financial stability experts could support in taking action to make the financial system more resilient to money laundering issues.

**MM:** A foundational step in addressing illicit financial flows is to understand the source of the main cross-border money laundering threats to the country and the financial flows analysis provides the toolkit to identify geographic money laundering exposures. We recommended to the countries with the most material flows in the region to monitor cross-border payments on the national level, which would facilitate more effective identification of evolving money laundering risks and suspicious payments and allow all AML/CTF agencies to better target areas of higher risk. While for a majority of the countries, the main money laundering risk from cross-border payments is illicit financial outflows, advanced and open economies in the Nordic-Baltic region are attractive for the integration of criminal proceeds from abroad, requiring an additional focus on AML/CTF regimes. This recommendation can be generalized to emphasize the importance of strengthening scrutiny of financial inflows in advanced economies and financial centers, which would also support anti-corruption, AML and good governance efforts worldwide. National money laundering/terrorist financing risk assessments around the world insufficiently analyze the cross-border money laundering/terrorist financing risks despite their importance, and we recommended that most countries in the region enhance their understanding of nonresident and cross-border money laundering/terrorist financing risks, incorporating data on economic linkages, such as trade and investment in the analysis.

**AT Europe:** *Machine learning, artificial intelligence (AI) and deepfake technology are being exploited by*

*criminals. How can financial institutions (FIs) stay ahead in combating money laundering/terrorist financing?*

**GJ:** Criminals are, indeed, increasingly using technology to further their activities. The illicit use of technology not only supports the commission of the predicate offense and subsequent efforts to launder criminal proceeds but can also interfere with the FI's ability to detect these activities and carry out effective AML/CTF preventive measures. For example, the use of deepfake technologies can directly interfere with an FI's ability to carry out customer due diligence measures by bypassing customer identification and verification controls. This isn't an excuse and just means that FIs must respond and adapt the controls that they are using. In designing AML/CTF controls, FIs need to understand the money laundering/terrorist financing risks and threats that they are facing. In this regard, they have a key advantage (over criminals) in their access to information. Sharing of information between AML/CTF supervisors and financial intelligence units (FIUs) is critical, along with information flow (e.g., details on typologies from FIUs, based on real cases, or "good practice" controls that supervisors have observed in other regulated entities) between FIs and these AML/CTF agencies. We are seeing the increasing use of public-private partnerships for this purpose, with some excellent examples in the Nordic-Baltic region. FIs may also need to look to further exploring their use of technology in order to prevent and detect money laundering/terrorist financing, but the starting point is to understand the risks/threats and the design of the AML/CTF framework (including the use of AI and machine learning) should follow.

**MM:** FIs were among the pioneers in using advanced statistical methods and machine learning for AML. Staying ahead means constantly enhancing the analytical toolkit to capture the evolving typologies and emerging risks. For example, even the most efficient

traditional rule-based systems for transaction monitoring have a very high level of false positives for suspicious transactions, requiring extensive manual validation. "Big data" on payments and the application of machine learning approaches—which can automatically adapt to evolving typologies—hold a significant potential for the efficient identification of patterns of suspicious transactions. In addition, AI can be a useful instrument in customer identification and verification as well as ongoing monitoring.

**AT Europe:** *What steps has the IMF taken in support of cooperation and information-sharing practices among banks across the world?*

**GJ:** Cooperation and information-sharing practices between AML/CTF agencies on a cross-border basis is one focus, and we have seen that the Nordic-Baltic region has a lot of good practices to learn from. In addition to participating in AML/CTF supervisory colleges (for specific cross-border institutions) and other international engagements, the IMF has a broader Nordic-Baltic AML/CTF Working Group that allows, on a regional basis, the exchange of information, knowledge and experiences gained on AML/CTF supervision. The project also examined the AML/CTF frameworks for the supervision of crypto-asset service providers (CASPs) and found early trends of regulatory arbitrage in the region. When we think of key priorities for cooperation and information sharing, this is an area that requires some attention. This is not just a Nordic-Baltic issue; countries around the globe need to figure out better ways to share sector-specific information, potentially through the establishment of a centralized network to exchange information about CASP authorizations, the scale of activity, and supervision. As part of the IMF Legal Department's AML/CTF capacity development work with countries, a project is underway to develop CASP risk-based supervision structures and tools (including supervisory money laundering/terrorist financing risk assessment)

in order to support each country's efforts to implement an effective AML/CTF framework.

**MM:** Considering the similarities in AML/CTF threats facing the region, Nordic-Baltic countries can effectively share information with one another regarding emerging cross-border threats and cooperate in identifying higher money laundering/terrorist financing risk countries, taking into account region-specific risk factors. This improved risk understanding can also be communicated to FIs, enhancing the effectiveness of AML/CTF preventive measures. Cooperation between the public and the private sector can also be explored in transaction monitoring, as the identification of suspicious transactions at the banking level may potentially miss activity that would look suspicious with a sector-wide view of patterns of payments. In addition, some data in the public sector—tax delinquency, for example—can be instrumental in detecting suspicious transactions, and technology might solve some of the operational and legal constraints.

**AT Europe:** *What can professionals working in the anti-financial crime industry do to deter money laundering/terrorist financing?*

**GJ:** Like we said earlier regarding the term "solving," "detering" is also a tough task. Criminals are looking to exploit weaknesses in the AML/CTF systems and the controls that banks have in place. So, when it comes to deterrence, it's about not giving criminals any ideas. What I mean is that a country's reputation for having a weak AML/CTF framework is clearly going to encourage criminals to look at the gaps, along with institutions that are subject to enforcement action (e.g., a published fine for AML/CTF failures). So, it comes back to making sure that there is a robust AML/CTF framework. In addition, the tone from the top and how institutions are perceived are also critical. Institutions that actively promote AML/CTF as a key strategic

priority and embed a culture of AML/CTF compliance will also serve to deter financial crime. These outward-looking components also mean that there are stronger and more robust internal AML/CTF systems and controls.

**MM:** If criminals know that a country monitors cross-border payments from the AML/CTF angle and can efficiently identify the suspicious payments patterns and the new typology, they might want to focus their laundering attempts elsewhere. Overall, a deterrence effect for transnational criminals can result from having an AML/CTF regime with effective mitigation of cross-border and nonresident money laundering risks, as shown, for example, in outcomes related to detection of and convictions for money laundering and asset recovery. Achieving these outcomes in cross-border money laundering for a deterrent effect requires not only effective international cooperation but also employing measures against professional enablers and autonomous money laundering, as well as enhanced scrutiny of nonresident and cross-border activity in advanced economies and financial centers that are the preferred destination for laundered money. **AT**

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

<sup>1</sup> "Nordic-Baltic Regional Report: Technical Assistance Report-Nordic-Baltic Technical Assistance Project Financial Flows Analysis, AML/CFT Supervision, and Financial Stability," *International Monetary Fund*, September 4, 2023, <https://www.imf.org/en/Publications/CR/Issues/2023/09/01/Nordic-Baltic-Regional-Report-Technical-Assistance-Report-Nordic-Baltic-Technical-538762>

<sup>2</sup> Pierre Bardin, Antoine Bouveret, Grace Jackson, et al., "Money Laundering Poses a Risk to Financial Sector Stability," *IMF Blog*, September 4, 2023, <https://www.imf.org/en/Blogs/Articles/2023/09/04/money-laundering-poses-a-risk-to-financial-sector-stability>



## MONEY LAUNDERERS FOR HIRE:

## ANTWERP'S COCAINE DILEMMA

In 2021, Belgian authorities intercepted a colossal 89 metric tons of illicit drugs valued at 4.5 billion euros (approximately \$4.8 billion) within the confines of Antwerp's bustling port in what was known as Operation Sky ECC. Despite the successful achievement and the apprehension of 888 suspects, the stakeout only scratched the surface of an expansive drug trafficking web that has taken a grip on Belgium.<sup>1</sup>

With its sprawling 130 square kilometers (50.2 square miles), the Belgian port of Antwerp has a reputation for being Europe's second-largest container terminal, as well as the leading port for cocaine seizures in the continent. Confiscations increased close to 21% between 2021 (91 metric tons) and 2022 (110 metric tons).<sup>2</sup>

The Belgian Financial Intelligence Unit (FIU), the Cellule de Traitement des Informations Financières (CTIF-CFI), published this year its 2022 activity report and revealed that the rise in Belgium's drug trade had boosted the need for specialists knowledgeable in money laundering techniques, paving the way for an explosion of money laundering as a service.<sup>3</sup>

Let us explore why criminal organizations in Belgium are seeking such services and what they offer.

### The entry point of cocaine

"The epicentre of the cocaine market in Europe has shifted northwards." With those words, Europol confirmed in its "Cocaine Insights" report that Rotterdam, Hamburg, and in particular, Antwerp, have taken over Spain as the leading entry points of cocaine into Europe.<sup>4</sup>

The market for cocaine has seen a surge in recent years due to Colombia's 2016 peace deal with the leftist Revolutionary Armed Forces of Colombia (FARC), who cultivated and regulated the access to cocaine supplies to international traffickers. Splinter groups formed from the ashes of the radical organization and forged alliances with European drug gangs who are now able to access shipments directly from the source without the need for previous middlemen.<sup>5</sup>

In Antwerp, Moroccan drug lords, Albanian kingpins and Italian 'Ndrangheta *mafiosi* have become the major players in the drug trade.<sup>6</sup> Their high degree of flexibility and mobility, their ability to operate internationally and their strength in joining forces allow them to reduce costs and maximize profits.<sup>7</sup>

While there are no precise figures on the amount of money generated by the cocaine trade in Antwerp, CTIF-CFI estimates that it is in the billions of euros based on recent confiscations.<sup>8</sup>

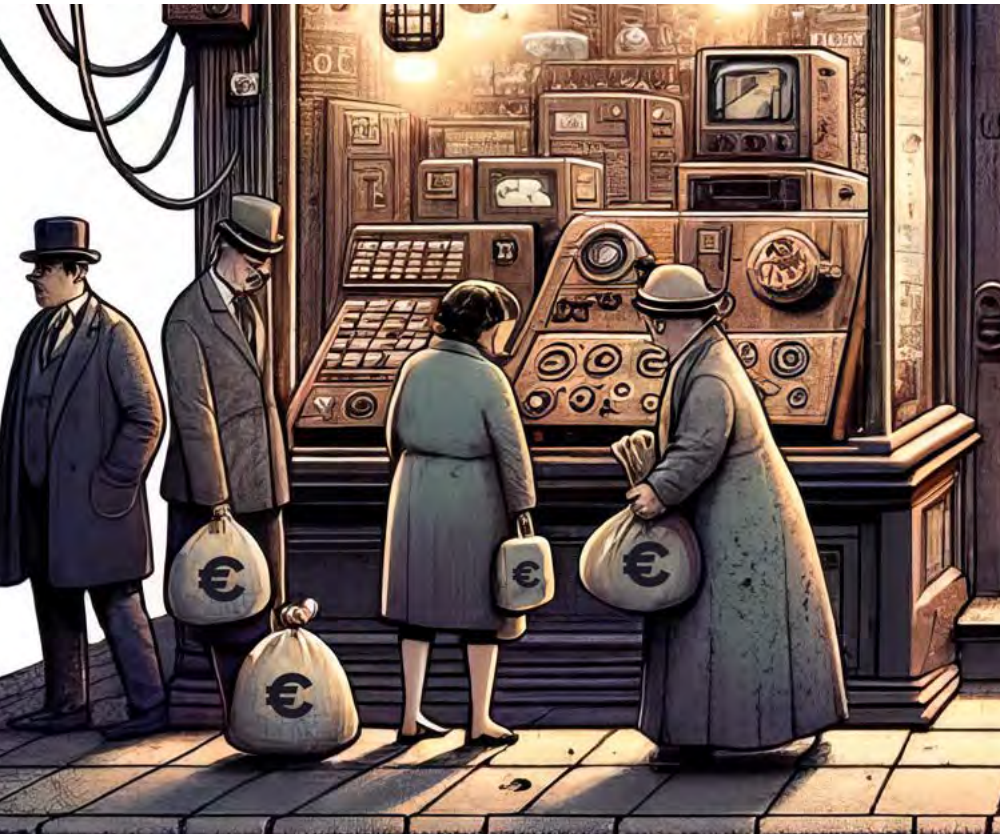
When it comes to hiding their assets, drug traffickers in Belgium are more concerned with masking their lavish lifestyles through legal façades such as commercial investments and front companies. The money laundering aspect is left to third-party professionals specialized in hiding and obfuscating the origin of their wealth.<sup>9</sup>

While CTIF-CFI's report does not present data on the amount of money laundering schemes as a service that were detected, it does state that there has been an increase in their use, particularly by drug traffickers.

### Money laundering on demand

Money laundering as a service, also known as professional money laundering (PML), is defined by the Financial Action Task Force (FATF) as a business, an individual or a network hired by a criminal organization to hide the nature, location, ownership, control, origin and/or destination of their illicit funds with the purpose of avoiding detection.<sup>10</sup>

CTIF-CFI has found that these professional networks have at their disposal numerous bank accounts, companies, money mules and frontmen, both in Belgium and abroad, to cover all three phases of money laundering. This may include



organizing the transport of the funds, moving them from shell companies to offshore accounts and investing them in real estate or luxury vehicles.<sup>11</sup>

The abuse of corporate structures by PMLs featured prominently in suspicious activity reports (SARs) sent to CTIF-CFI in 2022. Payment service providers (PSPs) were the ones to notify their frequent use of shell companies established in Belgium, as well as other enterprises set up in the European Union (EU). It was noted in CTIF-CFI's 2022 activity report that 80% of unlawful networks active in the EU use corporate structures for criminal activities.<sup>12</sup>

### A complex web of transactions

CTIF-CFI's report gives an example of a money laundering scheme conducted by a PML in Belgium.

The case involved various recently established Belgian companies, and all had registered offices in a business center. CTIF-CFI noted that they all had major inconsistencies and deficiencies in the ultimate beneficial ownership (UBO) register, such as recorded data that no longer corresponded to their current business situation.<sup>13</sup>

The analysis of bank accounts belonging to these companies revealed an increase in transaction magnitude that was attributed to management changes and the subsequent modification of the companies' operational activities.<sup>14</sup>

The amounts credited to the accounts of these Belgian companies originated from companies active in sectors different from theirs and sensitive to money laundering due to their cash-intensive nature, including construction, cleaning and transportation businesses. A large portion of the

credited amounts was then transferred to the accounts of various companies established in other EU countries and active in the beverage trade or mobile phone sales.<sup>15</sup>

Another portion was transferred to accounts held by European companies at a PSP. These entities seemed to serve as intermediaries for the final payment to companies in China. The money was sent from European companies to companies based in China to pay for the purchase of goods intended for convenience stores in Belgium, such as beverages and phones.<sup>16</sup>

Other payments were also sent to the accounts of law firms in the EU to finance the acquisition of real estate, thus creating a complex and varied web of transactions and purchases to hide the origin of the illicit money.<sup>17</sup>

### No light at the end of the tunnel

The rise of Antwerp's drug trade problem is in direct connection with the increase in demand for cocaine in the EU. It is now the second-most popular drug in Western and Central Europe after cannabis, with an estimated 4.4 million users in the past year.<sup>18</sup> Between 2021 and 2022, its usage rose 29% in Amsterdam, 28% in Brussels, 23% in Utrecht and 14% in Eindhoven.<sup>19</sup>

Substance trafficking is not the only issue. The rivalries between drug gangs have led to various acts of violence in and around Antwerp, including bombings, shootings and an attempted kidnapping in 2022 of the Belgian Minister of Justice, Vincent Van Quickenborne.<sup>20</sup>

The Belgian government is trying to squash the criminal syndicates by allocating 310 million euros to police forces and granting them further power.<sup>21</sup>

While confiscations continue, EU seaports administer around 90 million containers every year, but port authorities are capable of only inspecting 2% to 10% of them.<sup>22</sup>

Aside from law enforcement (LE), financial institutions (FIs) play a central role in disrupting the flow of cocaine in Belgium. In 2022, CTIF-CFI received a total of 53,923 SARs from FIs and information from foreign counterparts as well as government departments—a 71% increase in two years.<sup>23</sup>

Furthermore, it collaborates with its EU counterparts, transmitting information contained in SARs to the FIUs of countries mentioned in SARs thanks to European cross-border reporting procedures (XBRs). A total of 11,154 XBRs were transmitted in 2022.<sup>24</sup>

Despite the increase in vigilance, the scale of the problem remains daunting. Limited resources to inspect containers, associated violence, socioeconomic disparities, addiction and international drug trafficking networks not only mean that the issue will persist but that money laundering as a service will continue to rise, further complicating the fight against drug trafficking.

Sustained and comprehensive strategies, together with knowledge of the workings of money laundering as a service networks, could give an advantage to LE agencies and FIs in the uphill battle against Antwerp's cocaine dilemma. [AT](#)

Stefano Siggia, CAMS, senior consultant, Pideeco, Belgium, [stefano@pideeco.be](mailto:stefano@pideeco.be), [in](#)

- <sup>1</sup> Dylan Carter, "Belgian Minister of Justice Targeted in Suspected Kidnap Plot: What do We Know?" *The Brussels Times*, September 26, 2022, <https://www.brusselstimes.com/295952/belgian-minister-of-justice-targeted-in-suspected-kidnap-plot>
- <sup>2</sup> "The port of Antwerp," *Marvest*, <https://www.marvest.de/en/magazine/ships/the-port-of-antwerp/>; "Port of Antwerp welcomes officials following continued rise in cocaine seizures," *European Monitoring Centre for Drugs and Drug Addictions*, February 7, 2023, [https://www.emcdda.europa.eu/news/2023/port-antwerp-welcomes-officials-following-continued-rise-cocaine-seizures\\_en](https://www.emcdda.europa.eu/news/2023/port-antwerp-welcomes-officials-following-continued-rise-cocaine-seizures_en)
- <sup>3</sup> "Rapport d'activité 2022," *Cellule de Traitement des Informations Financière*, 2022, [https://www.ctif-cfi.be/images/documents/French/Rapports\\_annuels/RA2022FR.pdf](https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/RA2022FR.pdf)
- <sup>4</sup> "Cocaine Insights 1," *Europol and the United Nations Office on Drugs and Crime*, December 6, 2021, <https://www.europol.europa.eu/cms/sites/default/files/documents/cocaine-insights-1.pdf>
- <sup>5</sup> "Belgium, Netherlands major cocaine hubs: Europol," *Euractiv.com and AFP*, September 8, 2021, <https://www.euractiv.com/section/global-europe/news/belgium-netherlands-major-cocaine-hubs-europol/>
- <sup>6</sup> *Ibid.*
- <sup>7</sup> "Rapport d'activité 2022," *Cellule de Traitement des Informations Financière*, 2022, [https://www.ctif-cfi.be/images/documents/French/Rapports\\_annuels/RA2022FR.pdf](https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/RA2022FR.pdf)
- <sup>8</sup> *Ibid.*
- <sup>9</sup> *Ibid.*
- <sup>10</sup> "Professional Money Laundering," *Financial Action Task Force*, July 26, 2018, <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandrends/Professional-money-laundering.html>
- <sup>11</sup> "Rapport d'activité 2022," *Cellule de Traitement des Informations Financière*, 2022, [https://www.ctif-cfi.be/images/documents/French/Rapports\\_annuels/RA2022FR.pdf](https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/RA2022FR.pdf)
- <sup>12</sup> *Ibid.*
- <sup>13</sup> *Ibid.*
- <sup>14</sup> *Ibid.*
- <sup>15</sup> *Ibid.*
- <sup>16</sup> *Ibid.*
- <sup>17</sup> *Ibid.*
- <sup>18</sup> "Belgium, Netherlands major cocaine hubs: Europol," *Euractiv.com and AFP*, September 8, 2021, <https://www.euractiv.com/section/global-europe/news/belgium-netherlands-major-cocaine-hubs-europol/>
- <sup>19</sup> Sarah-Taissir Bencharif, "And the cocaine consumption capital of Europe is ... Antwerp," *Politico*, March 22, 2023, <https://www.politico.eu/article/antwerp-drugs-europe-cocaine-consumption/>
- <sup>20</sup> Lauren Walker, "Drug trafficking gang threat in Antwerp Port assessed in new Europol report," *The Brussels Times*, April 6, 2023, <https://www.brusselstimes.com/444056/threat-of-drug-trafficking-gangs-in-antwerp-port-assessed-in-new-europol-report>
- <sup>21</sup> Dylan Carter, "Belgian Minister of Justice targeted in suspected kidnap plot: What do we know?" *The Brussels Times*, September 26, 2022, <https://www.brusselstimes.com/295952/belgian-minister-of-justice-targeted-in-suspected-kidnap-plot>
- <sup>22</sup> Lauren Walker, "Drug trafficking gang threat in Antwerp Port assessed in new Europol report," *The Brussels Times*, April 6, 2023, <https://www.brusselstimes.com/444056/threat-of-drug-trafficking-gangs-in-antwerp-port-assessed-in-new-europol-report>
- <sup>23</sup> "Rapport d'activité 2022," *Cellule de Traitement des Informations Financière*, 2022, [https://www.ctif-cfi.be/images/documents/French/Rapports\\_annuels/RA2022FR.pdf](https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/RA2022FR.pdf)
- <sup>24</sup> *Ibid.*



A soccer goalkeeper in a green uniform is diving to catch a ball in a stadium. The background shows a large crowd of spectators and a clear blue sky. The title 'MONEY LAUNDERING IN SOGGER' is overlaid on the image in a stylized green and yellow font.

# MONEY LAUNDERING IN SOGGER

**T**he sports world is highly dynamic, generating a vast amount of economic activity, both legal and illegal. In sports, the higher the profits, the higher the risk of money laundering. As shown in Graphic 1 on the next page, soccer is the biggest sport around the world, especially in terms of business profits. This article addresses illegal activity in the world of sports—and soccer in particular.

Graphic 1: Soccer is the largest sport in the world



Source: The Sumsuber<sup>1</sup>

The following are some of the different ways that money can be laundered through the sport of soccer.

- **Inflated agent fees:** This is when agents overcharge their fees when representing players.
- **External activities:** Activities such as charity games—where a nongovernmental organization (NGO) receives funds that are meant to be distributed to organizations selected by a player—can be prone to money laundering when the funds are distributed, or not, to the respective NGOs.
- **Player image rights:** Image rights are another technique that can be used to launder money. The clauses in Lionel Messi’s contract are one example. Through these clauses, Messi receives a percentage of the revenue from Inter Miami jersey sales as well as revenue from his games watched on Apple TV.
- **Ticket sales:** Tickets sold in stadiums or over the internet can also be used to launder money within the sport.
- **Player transfers:** Transfers between teams can also be used to mask money laundering.
- **Online betting apps:** Betting apps can also be a source for enabling money laundering.

The Financial Action Task Force (FATF) claims that sports like soccer, basketball, volleyball and car racing are prone to money laundering due to the large sums of money handled in cash. These sports involve player transactions, sports club structures and more.<sup>2</sup>

In the article “Is there a relationship between money laundering and sports?” the author claimed that nine executives and five businessmen were indicted on charges of bribery, fraud and money laundering in the FIFA corruption scandal that came to light in the second half of 2015. Research shows that the bribes associated with the case, which totaled \$150 million, sought to influence sponsorship contracts for the FIFA-organized competitions CONCACAF and CONMEBOL that were held in the U.S. and South America.<sup>3</sup>

Cases like this are commonplace and reflect the vulnerability of the sports sector in general to money laundering. Its scope must be calculated in terms of the size and structure of the industry, whether the criminal activity is local or international and, of course, by the number of transactions that happen each day. These are all important details. Lack of ethics, the common denominator in all these situations, makes monetary inconsistencies difficult to be traced and calculated.

In recent months, the public has witnessed significant changes in soccer, such as Messi’s switch to Inter Miami. Messi’s contract, which is similar to the contract David Beckham signed in 2007, was designed in a highly peculiar fashion, giving Messi a much lower salary than the offers made by soccer teams from the Middle East.<sup>4</sup> Beckham’s \$250 million

contract revolutionized Major League Soccer as it gave him rights to purchase a team within the league. Messi’s contract also gives him that option. In addition, Messi will have rights as a content creator and will receive a percentage of clothing sales and broadcast rights with Apple TV. Image rights and content creator rights are precisely those that pose a risk of money laundering in complex contracts such as these, “through sales of media rights, and merchandise, players may not declare part of the money received, the money received settles in a tax haven.”<sup>5</sup> Although they might be highly creative ways to retain talent, these clauses represent a great risk for money laundering as they make monetary discrepancies difficult to detect.

### Conclusion

Many organizations need an oversight and notification system to halt the expansion of illegal money in soccer. This is true, particularly when buying and selling sports teams, where criminals often find institutions with weak oversight that allow them to launder money and expand their money laundering networks. For soccer, FIFA and other sporting institutions must update their oversight mechanisms to reduce money laundering through their institutions as there is no significant oversight at present and this affects the sport itself as well as its image. [AT](#)

**Carlos G. Cabrera, founder, co-chairman, CYGMA Capital LLC, carlosgcabrera@gmail.com**

<sup>1</sup> Alyssa Abrams, “How Money Is Laundered Through Football,” *The Sumsuber*, October 28, 2022, <https://sumsub.com/blog/money-laundering-football/>  
<sup>2</sup> “Money Laundering through the Football Sector,” *Financial Action Task Force*, July 2009, <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML%20through%20the%20Football%20Sector.pdf.coredownload.pdf>  
<sup>3</sup> Ana Mari Perea, “¿Existe relación entre el lavado de activos y el deporte?” *Tusdatos.co*, <https://www.tusdatos.co/blog/existe-relacion-entre-el-lavado-de-activos-y-los-deportes>  
<sup>4</sup> Paul Tenorio, “How Beckham’s transformative MLS contract paved the way for Messi,” *The Athletic*, July 10, 2023, <https://theathletic.com/4674349/2023/07/10/messi-miami-beckham-money/>  
<sup>5</sup> Alyssa Abrams, “How Money Is Laundered Through Football,” *The Sumsuber*, October 28, 2022, <https://sumsub.com/blog/money-laundering-football/>

# LOOKING FOR MORE ACAMS TODAY CONTENT?

Visit **ACAMSToday.org!**



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



# UNDERSTANDING GEOGRAPHIC MONEY LAUNDERING RISK

**A**nti-financial crime (AFC) regulations worldwide require that regulated businesses assess the business risk from money laundering, terrorist financing and proliferation financing perspectives. An important component of financial crime risk assessment is understanding and assessing the risk emanating from the geographies where business deals are conducted. This article addresses the geographic risk assessment, its meaning and the best practices to carry out the risk assessment.

## Geographic risk assessment from a financial crime risk perspective

The geographic risk assessment is the objective and independent assessment of money laundering/terrorist financing and proliferation financing risks associated with countries where business deals are conducted.

The geographic risk assessment must take into account various financial crime risk factors from domestic and cross-border sources, such as a specific jurisdiction's

national risk assessment (NRA) as well as publications by international organizations like the Financial Action Task Force (FATF).

## Why assess geographic money laundering risk?

It is when a business deals with an individual or a business in a foreign country that it exposes itself to various types of money laundering, terrorist financing and proliferation financing risks emanating from that geography. The regulated business must assess such risks and deploy suitable controls to counter, document and monitor them from an AFC compliance perspective.

Geographic risk alone does not determine the risks associated with a customer. One needs to take into account various risks originating from the nature of the product/service involved in the business relationship, the complexity of the transactions, the delivery and distribution channel used, as well as other relevant factors, to arrive at the overall risk associated with a customer.

The following are circumstances that require a geographic risk assessment:

1. When a regulated entity wants to enter into a business partnership with another entity or individual, it must carry out a geographic risk assessment
2. When a business establishes a business relationship with an individual or an entity
3. When an entity carries out an occasional transaction with an individual or an entity where there is no continuing relationship
4. When a regulated entity has a correspondent banking relationship with an overseas bank
5. When an entity outsources the customer due diligence (CDD) function to an overseas entity (relying on a third party for the CDD process)
6. While conducting the enterprise-wide risk assessment (EWRA)
7. When determining the customer's risk profile
8. When designing and developing the anti-money laundering (AML), counter-terrorist financing (CTF) and counter-proliferation financing (CPF) program

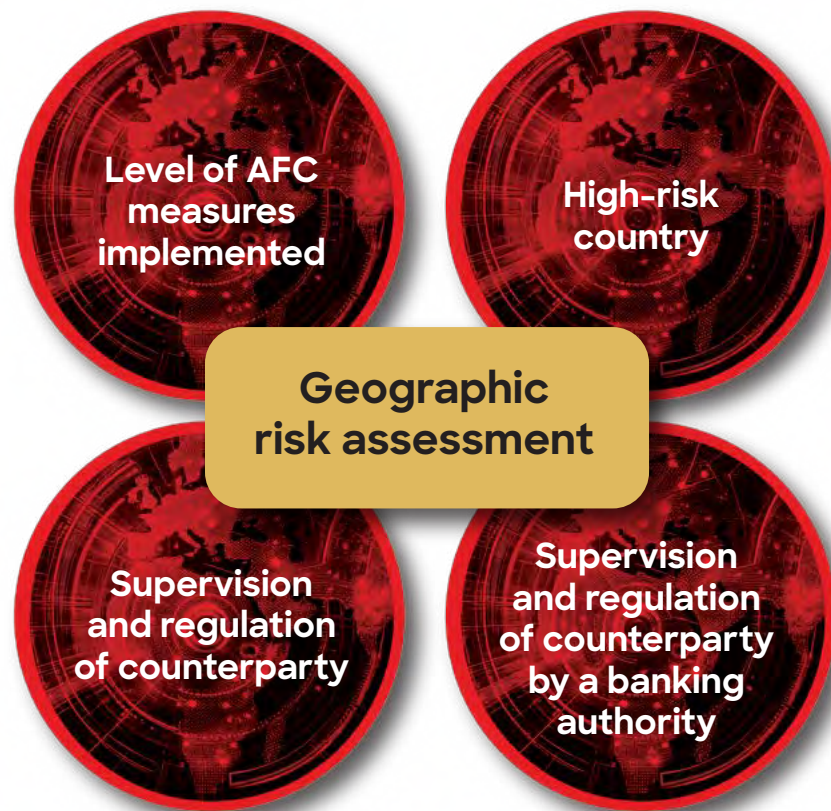


### Important factors to consider while performing geographic risk assessments

There are various types of factors to consider while performing geographic risk assessment. This is the list of the most important ones, which are visualized in Graphic 1:

1. Whether the country has implemented sufficient AFC measures
2. Whether the country under assessment is a high-risk country known for active connection with terrorism or proliferation
3. Whether the counterparty is supervised or regulated for AML and CTF purposes in the home country
4. Whether the counterparty is supervised or monitored by a banking authority in another country

Graphic 1: Important factors for performing geographic risk assessments



Visualization by Pathik Shah

### Risk-based approach

A business should adopt a risk-based approach (RBA) and focus on deploying more resources where the risk is greater. It should assess the probability of it being used for money laundering and terrorist financing purposes because of the jurisdiction with which it deals.

### How to determine if the country has implemented sufficient AFC measures

The business must determine if the country it is dealing with has implemented sufficient risk mitigation measures to fight money laundering, terrorist financing and proliferation financing. The following is a list of factors that can help determine if the country has implemented sufficient AFC measures:

1. The country has enacted AML, CTF and CPF laws.
2. The AML regulatory framework of the country requires financial institutions (FIs), designated non-financial businesses and professions (DNFBPs), virtual asset service providers (VASPs) and other high-risk businesses to prepare and implement AML/CTF programs, carry out CDD, transaction monitoring, identification and reporting of suspicious transactions, compliance with targeted financial sanctions regimes and meet record-keeping requirements.
3. The country has a proper governance structure to supervise regulated entities.
4. Check if the country under assessment is a member of the FATF or FATF-Style Regional Bodies (FSRBs).

### How to determine if the country under assessment is a high-risk country

While performing an EWRA, due consideration to the countries you deal with needs to be provided. The countrywide composition of the customers, suppliers and third parties you engage with needs to be verified. Further, when you perform a customer risk assessment, you need to consider the geographic risk associated with the customer.

There is no common definition of a high-risk country. However, you need to take into consideration the following factors to determine if a country is a high-risk country:

1. Countries subject to sanctions by United Nations Security Council Resolution
2. Countries sanctioned by a competent authority in the home country
3. Countries sanctioned by a competent authority in the foreign country where your business is conducted
4. Countries covered by the FATF list of high-risk jurisdictions subject to a call for action (blacklist)

5. Countries covered by the FATF list of jurisdictions under increased monitoring (grey list)
6. Countries identified by credible sources as countries supporting money laundering or terrorist activities
7. Countries suffering from high levels of corruption
8. Countries where the beneficial ownership of businesses is difficult to establish, and there are no regulations or deficient regulations to identify beneficial owners
9. Countries identified by credible sources as being tax havens
10. Countries that are involved in the production and distribution of illicit drugs
11. Countries suffering from high levels of other predicate offenses
12. Countries involved in the production, trading and distribution of weapons of mass destruction or proliferation financing
13. Search for the country under consideration in the Basel AML Index,<sup>1</sup> as shown in Graphic 2

Graphic 2: Sample view of the Basel AML Index

Income		Region		Search for jurisdiction <input type="text"/>	
<input type="checkbox"/>	East Asia & Pacific	<input type="checkbox"/>	Europe & Central Asia	<input type="checkbox"/>	Latin America & the Caribbean
<input type="checkbox"/>	Middle East & North Africa	<input type="checkbox"/>	North America	<input type="checkbox"/>	South Asia
<input type="checkbox"/>	Sub-Saharan Africa				
5	Madagascar				7.59
6	Guinea-Bissau				7.53
7	Cambodia				7.36
8	Mali				7.28

Source and visualization by Basel Institute on Governance<sup>2</sup>

### How to determine if the counterparty is supervised or regulated for AML/CTF purposes in another country

In order to determine if the counterparty is supervised or regulated for AML or CTF purposes in another country, you need to have a thorough understanding of the legal framework and supervisory authorities of the country being assessed. The evaluations made by FATF and FSRBs provide a lot of insight into this aspect. Here are some of the factors to determine if the counterparty is supervised or regulated for AFC purposes in the other country:

- Assess if the counterparty is supervised or regulated by a governmental authority acting as a supervisory authority for AFC purposes
- Check if the counterparty is duly registered with the supervisory authority
- Check if the supervisory authority is regularly monitoring the counterparty

### How to check if the counterparty is supervised or monitored by a banking authority in another country

Generally, AML regulations prohibit the regulated entities from entering into a business relationship with shell companies, banks and FIs. It is the responsibility of the business to prevent a single transaction with such shell entities.

1. Check if the counterparty possesses a trade license certificate of incorporation issued by the competent authority
2. Check if the counterparty has a physical place of business. You may insist on having a utility bill, property lease agreement or similar document
3. Check if there is an independent supervisory authority to regulate banks and FIs in the country under consideration
4. Check if a supervisory authority supervises the banks and FIs—say, the central bank
5. Check if the monitoring process by such independent authority is sufficient, considering global best practices

### Geographic risk assessment methodology

The regulated businesses must document their risk assessment methodology. FIs, DNFBPs and VASPs can employ a variety of sophisticated models and approaches to assess geographic risk.

It is up to the regulated businesses to determine the type and extent of the risk assessment methodology as per the nature and size of their business and the RBA adopted by them.

Keep the following best practices in mind when conducting geographic risk assessments:

1. The geographic risk assessment methodology should consider qualitative and quantitative information for risk identification, assessment and control implementation
2. The geographic risk assessment needs to be aligned with the RBA the business adopts
3. The geographic risk assessment must reflect the approved AML/CTF risk appetite
4. The geographic risk assessment must consider inputs from internal sources, compliance officers, independent auditors and various departments like risk management and internal control
5. The geographic risk assessment must take into consideration external information such as emerging money laundering and terrorism financing trends, sectoral risks, the NRA, the topical risk assessment and guidance from supervisory authorities, FATF, the Egmont Group and other competent authorities
6. The methodology must describe the classification and prioritization of risks and the weighing of risk factors
7. It should evaluate the probability of a risk materializing and its timing and impact on the business
8. It should evaluate various controls and their effectiveness in mitigating the geographic risk
9. It should determine the effectiveness of the AML and CTF measures
10. It should determine the net risk as a result of gross risk as reduced by various controls implemented by the business

11. It should determine the additional controls required to bring net risk or residual risk within the entity's risk appetite
12. It should list the various circumstances requiring manual overrides in risk evaluation and approval requirements for the same
13. It should be adequately documented, maintained, updated and communicated
14. It must be tested and audited for its effectiveness and compliance with regulatory requirements

### How to deal with high-risk geographies

Once you classify countries into low, medium and high risks, the question arises: How to deal with such high-risk geographies? Here is the approach that you can take while dealing with high-risk countries:

- You must maintain a list of high-risk geographies identified by your business
- Your AFC compliance program must specify the methodology for identifying and maintaining high-risk countries
- You must have detailed procedures in place for dealing with high-risk countries
- If a foreign customer is hailing from a high-risk country, you must conduct an enhanced CDD process as per the RBA adopted by your business
- You must maintain records for at least five years or more, depending on the regulatory requirements
- You must put specific countermeasures as advised by the country's supervisory authorities or the financial intelligence unit

EWRA is a critical part of creating an effective AFC program, following the company's RBA. Within an EWRA, the assessment of risks in different jurisdictions is a key component. It assists in tailoring the control measures to match the specific risks present in each location. [AT](#)

*Pathik Shah, CAMS, founder, NIYEAHMA Consultants LLP, Gujarat, India, [pathik@niyehma.com](mailto:pathik@niyehma.com), [in](#)*

<sup>1</sup> "Basel AML Index," *Basel Institute on Governance*, <https://baselgovernance.org/basel-aml-index>

<sup>2</sup> "Global ranking in 2022," *Basel Institute on Governance*, <https://index.baselgovernance.org/ranking>



**FIs, DNFBPs and VASPs can employ a variety of sophisticated models and approaches to assess geographic risk**

# Combating sanctions evasion





Sanctions compliance officers today are living in tumultuous times. Ask any group of sanctions compliance officers what has been keeping them busy and one response is likely to come up quite often: Sanctions against Russia.

While not subject to comprehensive sanctions, Russia has become “the most sanctioned country” today, overtaking Iran in less than two years. According to data compiled by Castellum AI,<sup>1</sup> as of July 14, there were approximately 16,000 targets sanctioned under the Russian sanctions programs by the U.S., EU, U.K. and several others from the Group of Seven (G7) economies. In contrast, Iran, which has been subject to sanctions since 1979, came in at a distant second with close to 4,000 targets. The complexity of the Russian sanctions is also unprecedented. Sectoral and activity-based sanctions, such as those restricting the number of deposits and sale of banknotes and the Russian oil price cap scheme, are innovative and not seen in past sanctions programs.

The Russian sanctions developments are also a watershed moment from two fronts. First, they have turbocharged the general awareness of sanctions and the risks they pose internationally. Unlike other sanctioned countries like North Korea and Iran, Russia had a larger and more globally connected economy and significant trading ties with the

EU and other economic blocs when the Russia-Ukraine war occurred. Hence, the imposition of Russian sanctions had a more readily felt impact by more countries and commercial enterprises worldwide. There is also significant mainstream and social media coverage of the Russia-Ukraine war, including its impact on livelihoods and the actions taken globally by governments and companies in response, such as sanctions or decisions to exit markets. Given the emotional nature of the subject and its relevance, such media coverage has greatly piqued the interest of the general public. A company’s actions or commercial decisions concerning the war can invoke strong emotions (positively or negatively) from the wider public, especially if sensationalized and reported by the media. The need to consider reputational risks in addition to legal and compliance risks in managing the impact of the Russia-Ukraine war has become absolutely critical.

Second, sanctions against Russia have increased geopolitical fractures, changed how governments design and use sanctions to achieve their intended effect and increased their focus on enforcement. While there was an overwhelming majority in how the world thought about or acted toward North Korean and Iranian sanctions, the situation is very different for Russian sanctions. There are countries or states that support the sanctions, there are those against the sanctions, others remain neutral and several others that go in

between these three positions. Because of this geopolitical complexity, sanctions-imposing countries had to change their approach, navigating between seeking to impose maximum costs on Russia and balancing the need to manage diplomatic and economic relations with other countries. As a result, there has been an astronomical increase in the number and variety of sectoral or activity-based sanctions imposed on Russia, which are more complex and difficult to monitor or implement than traditional list-based or comprehensive sanctions, as well as previous sectoral sanctions. Due to such sanctions “design innovation” reached a saturation point and because of the complexities with implementation, sanctions-imposing countries are likely to shift focus toward enforcement of preexisting Russian sanctions to ensure their effectiveness. In addition, increased enforcement may help the sanctions-imposing countries influence other countries or states that are against or have been neutral toward Russian sanctions.

As a result of these two broad trends, the risks associated with engaging in or facilitating potential sanctions evasion have significantly elevated. Sanctions compliance officers increasingly need to consider and manage sanctions evasion risks to protect their institutions. The following are some areas that sanctions compliance officers may want to consider.

### Investigative controls

Uncovering potential sanctions evasion requires sanctions compliance officers to keep abreast of prevailing sanctions evasion typologies and red flags, analyze how such red flags may translate to observable customer or transaction characteristics or patterns, and devise controls to select such characteristics and patterns for further in-depth review or investigation. This intuitively differs from sanctions screening, another important, fundamental control and cornerstone of most sanctions compliance programs that most sanctions compliance officers are familiar with and have focused on. Traditionally, such analysis and monitoring activities have rested with the anti-money laundering (AML) investigations or transaction monitoring teams in banks. Such investigative monitoring is also typically performed on a post-facto basis and a selected sample of customers and transactions due to the effort and depth of review required and the need to look at aggregated data and patterns or trends, which take time to form. In contrast, sanctions screening is usually performed on a pre-processing basis as much as possible, with coverage extending typically to activity that can be screened as well as analysis and review performed on an individual transaction or trigger basis. Important distinctions between sanctions screening and sanctions investigations are detailed in Table 1.

Table 1: Key differences between sanctions screening and sanctions investigations

Factor	Sanctions screening	Sanctions investigations
When performed	Mostly pre-processing	Mostly post-processing
Control coverage	Wide scope. Typically, no threshold is considered	On higher risk areas or on a sampling basis
Analysis coverage	On a transaction/alert basis	On aggregated data or historical activity/trend
Analysis focus	Used typically to decide if alerts are true or false matches or if there are risks of activity and compliance with applicable laws and regulations	Typically used to decide if there are elements of suspicion and if activity could be indicative of potential sanctions evasion

Sanctions compliance officers need to think about how to embed investigative controls into their sanctions compliance programs to combat sanctions evasion. This can be achieved by leveraging the existing investigation/transaction monitoring controls in the AML or wider financial crime program, with the sanctions compliance officers’ expertise on the typologies, red flags and monitoring scenarios or requirements. Alternatively, the sanctions compliance officers will need to consider developing such investigative capability within their teams. Given the political element of sanctions, which makes them slightly different from other facets of financial crime, their increasing complexity as well as the rapid pace of development may be worthwhile for sanctions compliance officers to consider the latter option for longer-term benefits and sustainability.

The outputs from investigative controls can also complement sanctions screening controls, where individuals and entities identified to be of concern from the investigations can be added to screening filters to systematically identify further potential exposures of customers or activities associated with these names.

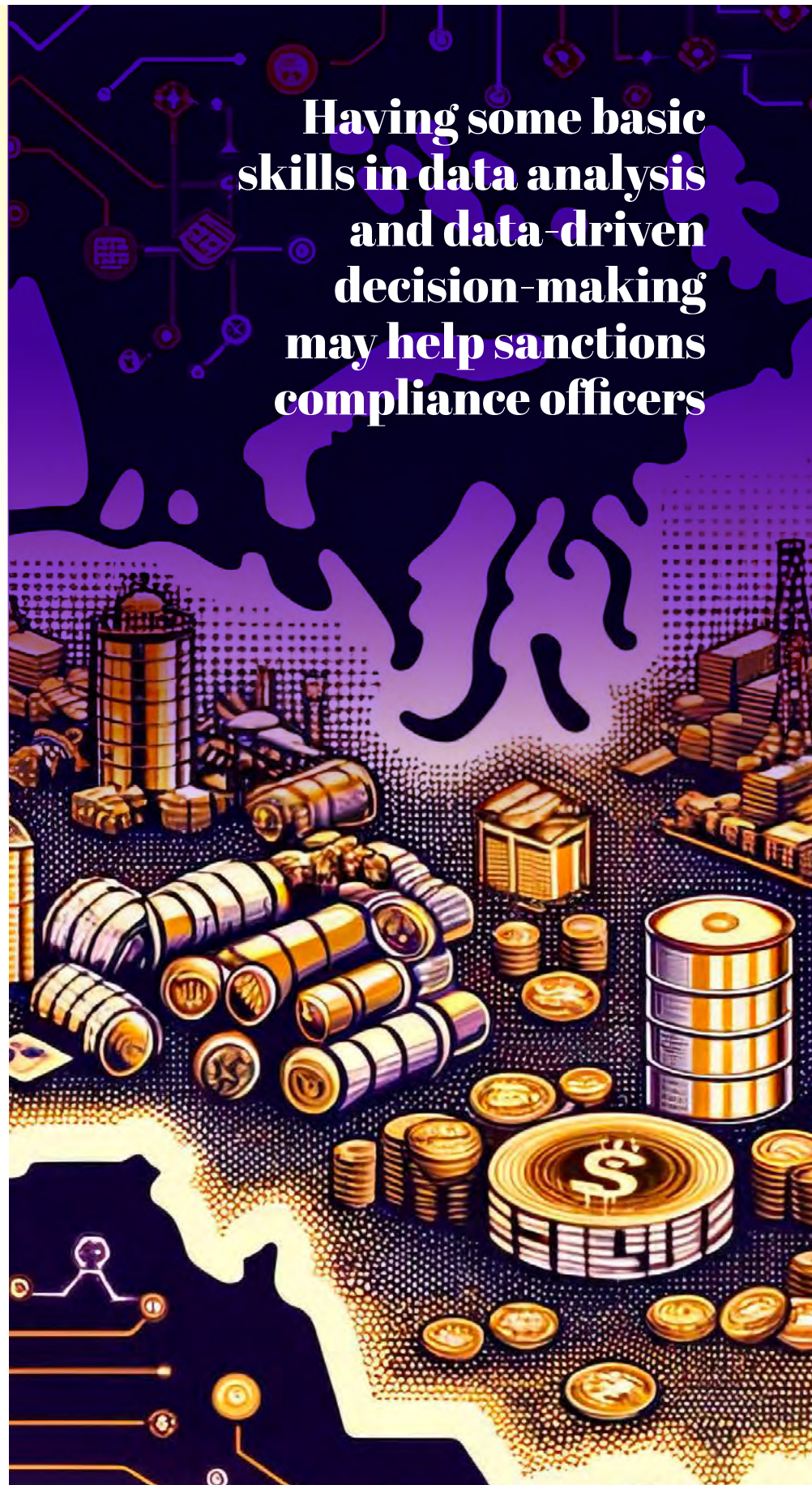
### Data-driven decision-making

Given the complexity and depth involved in investigative work and the limited compliance resources, sanctions compliance officers should consider implementing investigative controls in a consistent, repeatable manner with the highest chances of yielding results. Having some basic skills in data analysis and data-driven decision-making may help sanctions compliance officers.

Thinking about the critical data points associated with a typology or red flag, the analysis that can be performed on such data, and which outcomes or analysis results from the data are indicative of potential sanctions evasion can help guide investigative efforts for more consistent outputs as opposed to relying on the risk acumen and experience of individual analysts. Data analysis can also help identify higher risk samples for an investigation to concentrate limited resources for higher chances of success.

For example, a sanctions compliance officer may be interested in looking into the customer transactions that had passed his bank's screening filters but were subsequently rejected by the bank's correspondents for sanctions concerns, leveraging the correspondents' intelligence to identify customers that could be engaging in activities with unknown sanctions nexus or indicative of sanctions evasion. Rather than picking random samples, the sanctions compliance officer may consider the data points relevant to specific typologies to be covered under his review, such as the industry type of companies involved, goods/services traded, geographies involved, currency and products relevant to these

## Having some basic skills in data analysis and data-driven decision-making may help sanctions compliance officers



typologies. This can help the sanctions compliance officer derive a more risk-targeted subpopulation of customers with rejected transactions, whose samples can then be picked for in-depth review. Instead of looking at only large-value transactions for the sampled customers, the sanctions compliance officer can also use statistical analysis, such as anomaly detection by calculating standard deviation or peer analysis comparison, to further narrow down the past transactions of the sampled customers to request documents and other supporting information for further investigation. Data visualization tools can also help the sanctions compliance officer detect other customers with significant dealings or commonalities with the customers identified to be of concern from the initial reviews.

The sanctions compliance officer may not have the technical skill-sets to perform the actual data analysis or data visualizations themselves, but having the basic concepts and appreciation of a data-driven approach to problem-solving to be able to design or guide the investigation approach would be beneficial.

### Driving a strong compliance culture and risk awareness

While the above-mentioned second line of defense-driven controls and reviews can uncover and mitigate potential sanctions evasion risks, the first line of defense plays a critical, if not more important role in detecting and reporting such potential risks. Relative to compliance, the first-line business units often possess a deeper understanding of the customer's profile and activities and the transactional or market norms of the customer's industry. When armed with proper knowledge of sanctions risks and evasion red flags, they can play a very crucial and

effective role in detecting potential customer red flags for further review and advice by compliance, enabling more timely mitigation of risks. The cooperation and support from the first-line business units are also essential to enable the effective performance of the sanctions compliance officers' initial reviews, given that these reviews often require them to engage customers in sometimes difficult or sensitive conversations and ask for data on past transactions that the bank may have already processed.

In training the first line of defense on the topic of sanctions and sanctions evasion red flags and risks, sanctions compliance officers must make the risks appear real and relevant to them. Instead of focusing on technical aspects of what the regulations dictate or the bank's internal policies and prohibitions, the training should also include real-life case studies, preferably from the bank's own customers or activities. The first line of business should be able to relate that sanctions developments can influence the behavior or commercial decisions of their customers and how that can, in turn, bring risks to the bank. They should be advised of the increased interplay between reputational risks and Russian sanctions risks, where it is no longer sufficient to consider only the legal and compliance aspects of sanctions in managing the bank's risk exposures so that informed decisions can be made.

The tone from the top has the most influential impact on the attitudes toward risk and the bank's compliance culture. Hence, sanctions compliance officers have a strategic role to play in helping to explain, influence and educate their senior management on the risks and implications of this complex topic, which falls under their specialist domain.

### Conclusion

Sanctions imposed on Russia have sent the world a message that no country or state is too big or strategic to be targeted. Due to the wide-ranging impact and relevance of such sanctions, new geopolitical fractures have emerged and there is wider public interest and awareness of countries and firms' actions or attitudes toward sanctions. The likelihood of enforcement by sanctions-imposing states on preexisting sanctions has also increased.

As a result, sanctions evasion risks have elevated and become increasingly important for sanctions compliance officers to manage. Detecting and mitigating sanctions evasion, which often flies under the radar, is challenging. To increase their chances of success, sanctions compliance officers will not only need to maintain their technical expertise and domain knowledge but also keep abreast of the rapidly changing regulatory developments and sanctions evasion typologies. They may also have to become a bit of a financial crime investigator, data analyst and a convincing storyteller. [AT](#)

*Kelvin Kairong Toh, CAMS, group head of Sanctions, First Abu Dhabi Bank, [in](#)*

*The views expressed are those of the author and do not reflect the official policy or position of his affiliated institutions.*

<sup>1</sup> "Russia Sanctions Dashboard," Castellum.AI, October 16, 2023, <https://www.castellum.ai/russia-sanctions-dashboard>

# Can smart sanctions achieve their intended goals?

“**T**argeted sanctions” also called “smart sanctions,” have become increasingly popular with foreign policymakers to pressure specific entities or individuals in a targeted nation while minimizing negative impacts on innocent civilians. The main objective of targeted sanctions is to influence the behavior of the targeted individual or entity without harming the wider population. The objective is to achieve desired foreign policy outcomes without relying on measures that could have disastrous humanitarian consequences. On the other hand, comprehensive sanctions have the potential to severely impact the population, resulting in a shortage of essential goods and services that cause serious economic damage to the sanctioned country. While targeted sanctions, in extreme cases, may only be considered as the final resort, they are increasingly being recognized as an efficient and ethical means to achieve foreign policy objectives. Smart sanctions are more nuanced and strategic for foreign policymakers who must balance their objectives with ethical concerns by specifically targeting entities or individuals that pose a risk to global security or human rights.

The following are some of the advantages of targeted sanctions:

- **Precision:** Smart sanctions are specifically aimed at particular people, entities or sectors, making it easier to target those who present threats without negatively affecting the population.
- **Effectiveness:** Smart sanctions can be more effective than comprehensive sanctions as they focus on the specific behavior or activities that sanctioning nations wish to discourage. This approach is more effective than blanket restrictions that may not affect the intended targets.
- **Legitimacy:** Smart sanctions are perceived by the international community to be more legitimate because they are narrow and do not cause unnecessary harm to a larger population.
- **Force:** Smart sanctions can be used as a form of pressure to influence the behavior of the target persons or groups. If a government is subject to smart sanctions, it might be more likely to change its behavior to avoid further sanctions.

However, there are also some flaws with smart sanctions:

- **Evasion:** Identified individuals or entities may attempt to avoid smart penalties by using front companies, intermediaries and other tactics to continue prohibited activities.
- **International cooperation:** Smart sanctions need international cooperation to be effective. Without support from other countries, sanctioned individuals or entities may simply shift their activities to countries not subject to sanctions.
- **Sanctions fatigue:** Overuse or frequent imposition of smart sanctions may lead to sanctions fatigue, where countries become resistant to using sanctions as a foreign policy tool.



There are various measures governments can adopt to impose targeted sanctions against individuals, organizations or entities that violate international law, human rights, as well as peace and security. Governments can, for example, enforce travel bans on individuals deemed a threat to national security, peace and stability or are involved in activities that violate human rights. In addition, governments may freeze the assets of individuals or entities engaged in illegal activities, including corruption, terrorist financing or money laundering. Governments may also impose arms embargoes to prevent the sale or transfer of arms to individuals or entities that pose a threat to peace and security. Visa restrictions may also be implemented to deny or revoke visas to individuals who threaten peace and security, human rights or democratic rights. Trade restrictions, such as export controls, can be imposed on persons or entities engaged in illicit activities or who pose a threat to national security. Further, governments can prevent companies, banks and financial institutions (FIs) from conducting business with individuals or entities involved in illicit activities or who pose a risk to national security.

### Bypassing targeted sanctions

Targeted sanctions are designed to limit and isolate individuals or entities that engage in illegal activity or pose a threat to national security and international peace. However, some methods can bypass these sanctions, and some of these methods involve using third parties, engaging in money laundering, bartering trade, using cryptocurrency and loopholes in the sanctions regime.

- The use of non-sanctioned third parties includes the creation of front companies or shell companies to perform transactions or business activities that hide the real identity of a sanctioned person or entity.
- Money laundering techniques can also be used without detection to move funds, often by multiple transactions in multiple jurisdictions.
- Barter trade is another method that allows the exchange of products or services without the use of currency, which can bypass financial sanctions and move goods across borders.
- Cryptocurrencies that are decentralized and not controlled by any government or an FI can be used to move funds around without detection due to their anonymity.
- Another method to avoid specific sanctions is exploiting loopholes in the sanctions regime, such as exemptions or lack of cooperation among countries.

Although targeted sanctions can effectively limit the activities of sanctioned individuals and organizations, they are not foolproof and can be bypassed with different means. Therefore, it is crucial for governments to continually review and update their sanctions regimes to ensure the sanctions remain effective in achieving their intended objectives and prevent individuals or entities from exploiting loopholes.

An example of an individual who was able to continue his activities despite being sanctioned is Babak Zanjani, an Iranian businessman. Zanjani was sanctioned by both the U.S. and the European Union in 2012 for allegedly helping Iran evade international sanctions by using a

network of companies to sell oil and access the international financial system. Following the imposition of sanctions, Zanjani reportedly transferred ownership of his assets to a network of entities and individuals based in Malaysia, which were not subject to sanctions. These entities continued to engage in oil trading and other activities on behalf of Zanjani, effectively bypassing sanctions and allowing him to continue his activities.<sup>1</sup> This case serves as an example of how sanctioned individuals can utilize non-sanctioned entities to continue their activities and evade the impact of targeted sanctions. Despite the sanctions, Zanjani was able to carry on his business by transferring his ownership to third-party entities, thereby underscoring the need for governments to monitor and prevent such practices in order to enforce sanctions effectively.

This practice of using third-party companies to avoid targeted sanctions is a widespread issue that poses a major challenge to the effectiveness of targeted sanctioned actions. The use of third parties allows the sanctioned parties to continue accessing banking and financial services while avoiding the risk of being caught by the authorities directly. This makes it difficult for foreign policymakers to fully enforce and achieve their desired targets with sanctions.

Preventing evasion by smart sanctions requires a multifaceted approach involving a combination of policy actions, enforcement mechanisms and international cooperation. Governments can implement different strategies, including thwarting the evasion of sanctions.

- **Robust surveillance and enforcement:** Governments can enhance their monitoring and enforcement mechanisms to ensure that sanctioned individuals or entities cannot use loopholes. This can involve using advanced technologies and information-gathering techniques to track illicit activities.
- **Strengthening international cooperation:** Sanctions regimes are the most effective when they are backed by international cooperation. Governments can collaborate to share information, coordinate actions and improve their enforcement capability to prevent sanctions evasion.
- **Targeting third-party facilitators:** Governments can also target third-party facilitators, such as FIs or front companies that provide support to sanctioned individuals or organizations. This can involve imposing penalties or fines upon these entities or subjecting their own set of sanctions.
- **Examining the ownership structure:** FIs are required to assess the ownership structures of the entities involved in the transactions or business activities of the sanctioned individuals or entities. This may help to identify the beneficial owner and the control person behind the front companies or shell corporations used to conceal their true identity.
- **Transactions pattern and history:** FIs should examine the history and past transactions of the individuals and entities concerned as they may reveal potential risks or warning signs.
- **Implementing a robust sanctions compliance program:** This includes a comprehensive sanctions compliance policy in addition to using a sanctions screening tool that regularly checks against the updated



sanction lists. Also, the staff should be trained in sanctions policies and procedures. The sanction compliance program should be regularly reviewed and updated to ensure its effectiveness.

- **Enhancing transparency:** Governments can increase the transparency of sanctions regimes by providing clear guidelines on the scope and the application of sanctions. This may help to prevent confusion and ensure that people are aware of the potential consequences of engaging in illicit activity. Also, staff should be encouraged to report any violations.
- **Regularly updating sanctions regimes:** Sanctions systems should be updated regularly by governments and sanctioning bodies such as the United Nations to ensure they stay effective in achieving their goals. This can involve adding new individuals or entities to the list or modifying the scope and application of existing sanctions.

### Conclusion

There has been a growing trend among foreign policymakers to use targeted sanctions to achieve their foreign policy goals in a more ethical and effective manner. By using these sanctions, desired behavior can be brought about while minimizing the impact on innocent civilians. However, even if targeted sanctions come with some challenges, such as the possibility of evasion, the need for international cooperation and the potential for sanctions fatigue, governments and sanctioning bodies must take a range of measures to impose targeted sanctions on individuals or entities that violate international law, rights or the peace and security of civilians. [AT](#)

Mohamed Abouzied, CAMS, CFE, CGSS, compliance advisory manager-Middle East & Africa, [mdyazan@gmail.com](mailto:mdyazan@gmail.com), [in](#)

<sup>1</sup> "Treasury Targets Network Attempting to Evade Iran Sanctions," U.S. Department of the Treasury, April 11, 2013, <https://home.treasury.gov/news/press-releases/j11893>

# Career growth:

## *The importance of self-training*

**T**raining is an often-misunderstood pillar of anti-money laundering (AML) programs. Some practitioners in the AML industry believe the requirement is for the training of all personnel in an organization when the requirement is actually “training for appropriate personnel.”<sup>1</sup> A deeper dive into the regulatory requirement for training will underscore why training yourself is important for your career growth.

### Why you should train yourself

There is no “one-size-fits-all” definition for training. Training can and does occur in a multitude of ways, from one-on-one coaching, attendance at webinars and conferences, reading industry magazines and white papers, to attending peer group meetings. The Federal Financial Institutions Examination Council’s (FFIEC) “BSA/AML Examination Manual”<sup>2</sup> states, in part, for banks: “Training should be tailored to each individual’s specific responsibilities, as appropriate.”<sup>3</sup>

Training should be tailored to meet each individual’s responsibilities. The manual goes on to state that certain business units may require targeted red-flag training. New employees should receive an overview of the purpose of the Bank Secrecy Act (BSA) and its requirements. In addition, the board of directors and senior management should receive “Foundational training and be informed of changes and new developments.”<sup>4</sup> The manual also states, “The BSA compliance officer and BSA compliance staff should receive periodic training that is relevant and appropriate to remain informed of changes to regulatory requirements and changes to the bank’s risk profile.”<sup>5</sup> What the manual does not state is a requirement for financial institutions to provide training to appropriate personnel to grow knowledge, which could aid in career growth. There is no regulatory obligation for your employer to provide AML training to increase your knowledge of BSA, AML, regulatory requirements or general risk and compliance concepts.

Your knowledge growth is your responsibility, not your employer’s obligation.





Understanding why you are performing the tasks you are performing is one of the most important questions you can ask. The answer to the question drives understanding of the risks faced and controls implemented. The answer to the question not only allows you to think outside of the box but also supports knowing when an entirely new box might be beneficial to the organization. Understanding why you are doing what you are doing not only benefits the company but is important to your professional growth.

When you have a strong sense of why you are doing the work you are doing, you have a clearer vision of the desired outcomes. The clarity of vision provides opportunities for insight that others simply will not have.

The knowledge resulting from training outside of your current responsibilities can lead to a multitude of benefits.

- Being selected for key assignments or projects
- Increased visibility to senior management
- Becoming the “go-to” person on the team
- Becoming more “recession-proof”

In the transformative economy experienced in the past four years, the final bullet above may be the most enticing reason for workers to want to enhance knowledge outside of their current roles.

Being a one-trick pony<sup>6</sup> is dangerous in a tumultuous economy.

### How to train yourself

Unfortunately, there is no universal training path. The path you take will be dependent on the role you currently have, the role you want to attain, the amount of time you dedicate to training, the amount of money you can dedicate to training, and your employer’s willingness to support your growth, among other unnamed factors. Table 1 below offers various methods to train yourself, ranging from no cost to those requiring a financial investment. It is important to think of training as an investment in your present (avoid downsizing) and future (career growth).

Table 1: Various methods of self-training

Training	Employer-related or industry-related	Cost
Learn regulatory requirements	Industry	\$
Read consent orders and social media influencers	Industry	\$
Read and understand your organization’s control documents	Employer	\$
Enhance your general knowledge of risks and controls	Employer	\$
Join industry groups	Industry	\$ - \$\$\$

#### COST KEY

\$	\$0 - low
\$\$\$	High



# 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](https://acams.org/sanctions)

**“Leadership wants to field the best team.... People with highly specialized skills that are hard to replace may be overlooked for dismissal, whereas workers that possess talents that are ubiquitous and easily replaced are not safe.”<sup>7</sup>**

Although many of the training options listed require minimal financial outlay, all the options require an outlay of time.

**Learn regulatory requirements:**

Generally, regulations are available for free on the internet. And you will likely find the regulations on multiple sites. You want to ensure you are selecting a source that is reputable (avoid wikis) and consistently updated. Once you have found a trusted resource, take your time. Do not try to rush the process. Do not take shortcuts. The regulatory requirements are the foundation for all the knowledge to follow.

**Read consent orders and industry influencer posts:**

Consent orders will provide information on how regulators apply regulatory requirements. Consent orders are found on each regulator’s website. For many regulators, you can register for email notifications of new regulatory actions. Do not forget to include the Office of Foreign Assets Control (OFAC) and the Financial Crimes

Enforcement Network (FinCEN) when registering for updates. Although technically not regulators, they both levy regulatory fines and penalties, and you will find benefit in reading these.

Reading posts by industry influencers provides a few benefits. It exposes you to different industries, risk tolerances as well as control options, and alerts you to impending rule changes. The trick here is finding the correct people and organizations to follow. You do not want to muddy your feeds with posts from individuals or organizations whose primary purpose of posting is exposure (e.g., they post inspirational quotes or public relations pieces). You want to follow influencers who have their thumbs on the pulse of the industry. By following social media influencers, you have the added benefit of being notified of upcoming remote and in-person training.

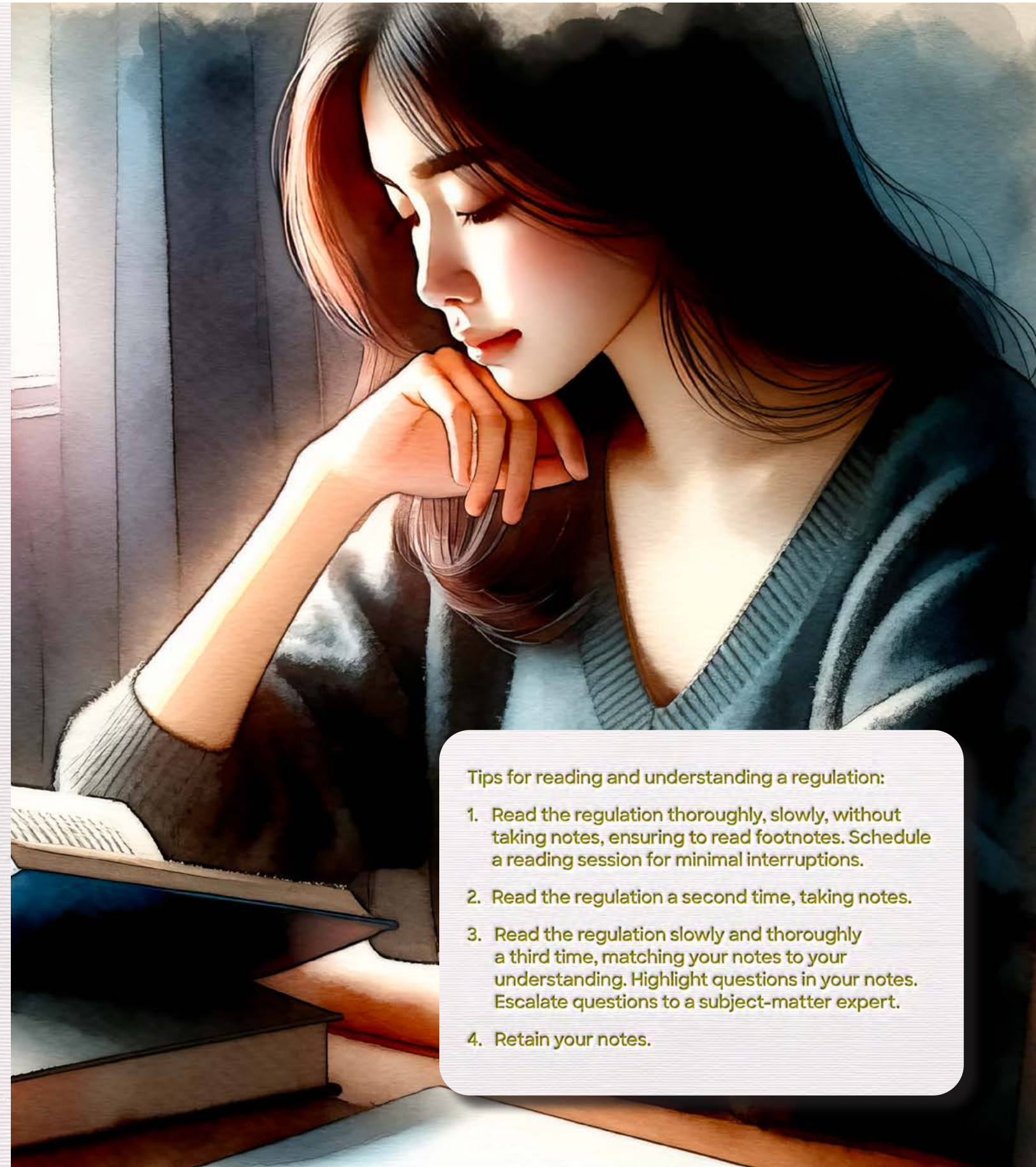
**Read and understand your organization’s control documents:**

Organizations vary how documents

are titled (AML program or policy,<sup>8</sup> BSA program or policy, standards, procedures, risk assessment, senior management reporting). From reading these documents, you will gain a deeper understanding of your organization’s processes, controls and risk tolerance. You will find out whether your organization has AML quality assurance programs or quality control programs.<sup>9</sup> You will discover which departments in your organization receive training. If you work for a bank, you will learn what enhanced controls are in place for higher (money laundering) risk customers.

**Enhance your general knowledge of risks and controls:**

You will gain some understanding of the controls by reading the governance documents. Be curious. Ask questions of teammates and other co-workers. Ask your manager for time to learn firsthand about processes with side-by-side sessions. Ask to attend meetings you would normally not attend—perhaps you can gain entry by



**Tips for reading and understanding a regulation:**

1. Read the regulation thoroughly, slowly, without taking notes, ensuring to read footnotes. Schedule a reading session for minimal interruptions.
2. Read the regulation a second time, taking notes.
3. Read the regulation slowly and thoroughly a third time, matching your notes to your understanding. Highlight questions in your notes. Escalate questions to a subject-matter expert.
4. Retain your notes.

offering to serve as the secretary taking minutes. Alternatively, ask your manager if he or she would be opposed to forwarding the minutes of project meetings in which you have an interest.

Seek out cross-training opportunities. If someone leaves the company, offer to fill in until the backfill is hired. Did a system upgrade result in an unexpected volume of alert types with which you have never worked? Offer to learn how to process them. Does the manager need an Excel macro? Figure out what is needed and get the job done. Cross-training is the foundation of being fungible. Fungibility is the foundation for becoming the “go-to” person on the team. Find a need and fill it.

Make the case for devoting time to attendance at external peer group meetings. Cannot find one that is at a convenient time? Start your own peer group meeting to be held during your lunch break. Be ambitious. Become so efficient in your daily work that you have time to dedicate to attending webinars. Find on-demand webinars to fit into your schedule. Sign up for live webinars. Oftentimes, links are distributed afterward to those who were not able to attend, ensuring you do not miss out on the information. You will be able to view the recording of the webinar at a later time that works for your schedule.

**Join industry groups:** Industry groups, like ACAMS, provide so many benefits, like access to thought leaders and networking. One of the things ACAMS does best is providing training on varied topics by industry experts delivered at a level suited to the topic and audience. There may be a cost to

joining industry groups and/or registering for some webinars. This financial investment opens doors to otherwise closed access, like proprietary publications (e.g., magazines, white papers). In addition, you may receive discounts on webinars or conferences. As a member of an industry group, you may be eligible to sit for certification exams offered by the organization. Access to topics you might not touch in your day-to-day world is not to be understated. Soak up information like a sponge soaks up water. You may not have a need for a specific piece of information today, but that does not mean it will not be helpful tomorrow. Avail yourself of all the benefits membership has to offer.

Realistically, completing the above steps can take many months or years. Training yourself is not a process to be taken lightly or to be hurried. Following the above guidance cannot guarantee that you will not be laid off or that you will receive that promotion you have been working hard to get. But it is likely that if you forge your own training path, your career path will follow. Knowledge is power. Knowledge provides confidence. Confidence breeds success. Start your training journey today. **AT**

*Amy Wotapka, CAMS, BSA and OFAC officer, First American Bank, USA*

- <sup>1</sup> “§ 1020.210 Anti-money laundering program requirements for banks,” *National Archives, Federal Code Regulation*, September 15, 2020, [https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-B/section-1020.210-1020.210a\(2\)\(iv\)](https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-B/section-1020.210-1020.210a(2)(iv))
- <sup>2</sup> Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual, *FFIEC Bank Secrecy Act/Anti-Money Laundering InfoBase*, <https://bsaaml.ffiec.gov/manual/Introduction/01>
- <sup>3</sup> “Assessing the BSA/AML Compliance Program, BSA/AML Training,” *FFIEC Bank Secrecy Act/Anti-Money Laundering InfoBase*, <https://bsaaml.ffiec.gov/manual/AssessingTheBSAAMLComplianceProgram/05>
- <sup>4</sup> *Ibid.*
- <sup>5</sup> *Ibid.*
- <sup>6</sup> One-trick pony definition and meaning, *Merriam-Webster*, [https://www.merriam-webster.com/dictionary/one-trick pony](https://www.merriam-webster.com/dictionary/one-trick%20pony)
- <sup>7</sup> Jack Kelly, “Here’s How To Avoid Getting Laid Off,” *Forbes*, June 16, 2022, <https://www.forbes.com/sites/jackkelly/2022/06/16/heres-how-to-avoid-getting-laid-off/?sh=2248ce78579a>
- <sup>8</sup> An AML program is different than an AML policy (though they may be combined to one document). In some organizations, the BSA program or policy may be a separate document from the AML program or policy.
- <sup>9</sup> “Quality Assurance vs Quality Control,” *ASQ*, <https://asq.org/quality-resources/quality-assurance-vs-control>

# ACAMS

## Enterprise: the Tool Your Financial Crime Prevention Team Needs

ACAMS Enterprise is a premium professional membership package for any organization involved in preventing financial crime.



### Why Enterprise?

- Provide your team members with all the benefits of ACAMS individual membership, plus **unlimited access to moneylaundering.com** and our entire webinar library
- Use **Enterprise usage reports** to track your team’s training and demonstrate compliance to regulators
- **Optimize your training budget**, with preferential rates for ACAMS training and events

Learn more here  
[www.acams.org/enterprise](http://www.acams.org/enterprise)





# Silas Bartels:

## Providing timely AFC analysis

**S**ilas Bartels is the legal editor of *ACAMS moneylaundering.com*. He manages a team of two attorneys that contribute to the publication's coverage of financial crime, sanctions and compliance-related issues. Complementing the breaking news and in-depth coverage of the talented reporters at *ACAMS moneylaundering.com*, his team provides timely analysis of enforcement actions, prosecutions and legislative and regulatory initiatives as they commence. His work also supports the *AFC Bulletin*, an ACAMS Enterprise premium resource that provides detailed analysis of regulatory and enforcement actions quarterly. Bartels joined ACAMS in 2014 as a part-time legal writer based in the New York office. This position built on his previous experience with the legal team of an international nongovernmental organization (NGO) and his academic writing on counterterrorism. He began his current role in September 2021. Bartels was born and raised in Santa Fe, New Mexico, before moving to upstate New York. A competitive academic intensive study and professional internship program brought Bartels to Manhattan in January 2013, and he now resides in Brooklyn.

**ACAMS Today (AT):** Describe what an average workday entails for you at *ACAMS moneylaundering.com*.

**Silas Bartels (SB):** Close collaboration between my team of attorneys and the talented reporters at *ACAMS moneylaundering.com* underpins our crucial work. Our standard day begins by exchanging important information, including regulatory and law enforcement developments. My team then analyzes, summarizes and publishes regulatory documents to complement the hard-hitting reporting of

the news team. In addition, we often collaborate on initiatives or projects with colleagues from other departments at ACAMS.

**AT:** What are some aspects of *ACAMS moneylaundering.com* that may not be well known to most people?

**SB:** In addition to *ACAMS moneylaundering.com* being the top source for news on financial crime, sanctions and compliance-related issues, the website has a range of useful functions for subscribers. I highly encourage members to sign up for our email alerts on breaking news items and the weekly wrap-up newsletters that cover a range of topics. *ACAMS moneylaundering.com* subscribers can also create custom email alerts to receive specific industry developments as they occur.

**AT:** In the past five years, which enforcement action has significantly impacted the anti-financial crime (AFC) industry?

**SB:** While it is challenging to choose one, I believe that the combined penalties of approximately \$2.3 billion against Denmark's Danske Bank<sup>1</sup> in December 2022 demonstrated a robust regulatory response against a foreign financial institution for deceiving U.S. correspondent banks. The actions by U.S. agencies marked the culmination of a yearslong regulatory response from supervisors across the globe. I think it is also fascinating to see a renewed regulatory focus on the cryptocurrency market due to the collapse of FTX and others last year.


**AT:** What AFC topics are you most passionate about and why?

**SB:** During my time at ACAMS, I have felt myself resonating with concerns that overly robust AFC and sanctions compliance measures may impede the flow of legitimate humanitarian aid to areas that most need it. I am pleased to see some progress in codifying humanitarian exemptions to sanctions last year, as well as recent revisions by the Financial Action Task Force to encourage risk-based and proportionate measures. I welcome the important work of my colleagues at ACAMS to promote best practices in AFC that promote financial inclusion and avoid unnecessary de-risking.

**AT:** Which aspect of your job do you most enjoy?

**SB:** I am very proud of the exceptional journalism of my colleagues at *ACAMS moneylaundering.com*, which includes frequent scoops and exclusive news items. It is extremely rewarding to support that work and other premium resources for ACAMS Enterprise members, such as the quarterly *AFC Bulletins*.

**AT:** What do you like to do in your spare time?

**SB:** When I have the time, I enjoy performances, street festivals and other events that occur here in New York all year round. My passion for cycling has also evolved from being a nice way to get out of the apartment during the COVID-19 pandemic to regularly participating in 50- to 100-mile events. 

Interviewed by ACAMS Today editorial, *ACAMS*, [editor@acamstoday.org](mailto:editor@acamstoday.org)

<sup>1</sup> "Danske Bank Admits US Bank Fraud Conspiracy," *ACAMS moneylaundering.com*, December 13, 2022, <https://www.moneylaundering.com/news/danske-bank-admits-us-bank-fraud-conspiracy/>



## ACAMS Pittsburgh Chapter: Education is the foundation for AFC

**F**ounding director of the Anti-Money Laundering (AML) Graduate Certificate Program and associate professor at Gannon University, Musa Tuzuner, spoke to the ACAMS Pittsburgh Chapter about his career, studying anti-financial crime (AFC) and incorporating the lessons learned from the field experience and the classroom setting into the AML field.

**ACAMS Pittsburgh Chapter (APC):** *When and how did you get into financial crime compliance?*

**Musa Tuzuner (MT):** After completing my undergraduate education at the police academy, I embarked on a fulfilling journey that led me into the realm of financial crime compliance. I began my career by joining Interpol's national bureau and intelligence department in Turkey, followed by serving in the United Nations' peacekeeping operations in Kosovo. Starting as a deputy captain, I eventually rose to the position of chief intelligence officer.

During my tenure in these critical roles, I developed a deep understanding of criminal and terrorist behaviors, including their involvement in money laundering and terrorist financing activities. This knowledge became the foundation for building effective preventive measures and policy recommendations to combat financial crimes.

As the chief intelligence officer in my jurisdiction, I focused on reducing terrorist activities, including addressing terrorist financing risks. Through innovative systems and methodologies that I developed and implemented, we successfully achieved an 80% reduction in terrorist activities, mitigating terrorist financing risks significantly. My work in this area earned me recognition as a "genius inventor" by the intelligence chief.

Despite these significant accomplishments in identifying risks and developing countermeasures on a national and international scale, I realized the need to enhance my research skills to further contribute to the field. I decided to pursue a doctoral education in the U.S., focusing on quantifying terrorist financing risks and studying counter-terrorist financing behavior. In addition, I aimed to understand why financial crime fighters perceive the real nature of terrorism financing risks and threats differently, even if they work in the same institutions.

During the subsequent years, I pursued various certifications, including those from ACAMS, to continuously develop innovative solutions that address identified gaps in the AFC sector.

My journey into financial crime compliance has been shaped by a commitment to making a real impact in combating financial crimes and mitigating the risks associated with terrorism financing. Through a combination of practical experience and advanced education, I strive to contribute to the development of effective systems and solutions in the AFC field. I believe that my current AML book project titled “Innovative Solutions for Anti-Money Laundering and Counter-Terrorism Financing” would be a great contribution to the field.

**APC:** *What was your inspiration to bring financial crime compliance into colleges and universities?*

**MT:** The inspiration to bring financial crime compliance into colleges and universities originated from my firsthand observations in national and international working environments, where I noticed that law enforcement and national security intelligence officers often perceived the nature of risks and threats differently due to various factors. This discrepancy led to different institutions devising separate solutions and countermeasure practices even when presented with the same risk information. Consequently, precious institutional resources were unnecessarily wasted.

Recognizing the importance of developing a unified and comprehensive approach to combat financial crimes, I realized that financial crime fighters must possess a mindset that truly understands the evolving nature of criminal and terrorist behavior. By fostering a culture of sharing, I successfully initiated innovative informal meetings with my staff and other stakeholders,

transforming their perceptions and institutional practices seamlessly. Through these efforts, we established an effective counter-terrorist regime in our jurisdiction, significantly mitigating terrorism risks. The journey to achieve this was time-consuming, and during that period, I wished that such critical knowledge would have been imparted at universities.

When I embarked on building academic programs and research centers, particularly in the U.S., I discovered that certain aspects I wished for had already been incorporated into intelligence education. However, I identified a gap in academic programs specifically focused on the AML field. Consequently, I decided to fill this void by creating an AML minor program within a leading intelligence program in the U.S.

Currently, I am furthering these efforts by developing a world-class AML graduate certificate program. My vision is to educate future AML talent intelligently, leveraging evolving public and private partnerships at both the national and global levels. Esteemed AFC professionals have described these endeavors as innovative approaches to reshaping the educational landscape and fostering a robust pipeline of future AML talent.

### **An effective AML professional possesses several key qualities and practices that contribute to their success in combating financial crimes**

**APC:** *Do you have any role models/mentors and if yes, please describe how they have shaped the professional you are today?*

**MT:** I have been incredibly fortunate to have had numerous role models and mentors throughout my career and education, each of whom has played a significant role in shaping my professional growth. Although it’s challenging to mention all their names in this limited space, I am deeply grateful for their invaluable support, guidance, encouragement and insights that have paved the way for my journey.

Among the many mentors who have influenced me, I would like to highlight three individuals who have had a profound impact on my professional development while I was in the U.S. First and foremost, Dr. Jim Breckenridge, whose mentorship has been instrumental in guiding me through challenges in educational institutions. He encouraged me to apply my innovative ideas about AML at Mercyhurst University, where I was able to initiate an AML program and other relevant activities. His guidance and support significantly shaped my leadership skills in the American context.

In addition, at my current institution, Gannon University, two individuals have played crucial roles in shaping my career. Dr. Walter Iwanenko, the visionary president of the university, impressed me with his leadership style, which inspired me to join Gannon University to build a world-class AML graduate education with institutional support. Without the unwavering support and insightful guidance of Julia Mack, associate dean for Curriculum and Student Affairs, I would not have been able to establish public and private AML partnerships, integral components of global AML education that include hands-on projects, professional tools and certification preparations.

The collective influence of these mentors and role models has instilled in me a drive for excellence and a commitment to making a meaningful impact in the field of financial crime compliance. I am immensely grateful for their support and encouragement, which have been instrumental in shaping the professional I am today.

**APC:** *What benefits do you feel a graduating student with a financial crime degree can offer an organization that is looking for the next AFC professional?*

**MT:** Drawing from my three decades of field and education experiences, a financial crime degree should aim to develop key skills and techniques that are currently in demand across all public and private sectors. Alongside professional certification preparations, integrating essential industry software tools into the education curriculum is imperative. This approach enables students to effectively investigate, analyze, identify and assess the financial crime risks faced by their institutions. In addition, establishing corporate partnerships can provide students with valuable opportunities, including scholarships, joint research projects, access to early career opportunities and professional development conferences.

A graduating student with a project-based financial crime education offers numerous benefits to organizations seeking skilled financial crime fighters. First and foremost, these students receive hands-on experience working on real-life cases involving money laundering, terrorist financing and crypto laundering. Their ability to create comprehensive reports, including link charts that illustrate the flow of illicit funds, brings fresh perspectives, up-to-date knowledge and a profound understanding of the evolving financial crime risks.

Secondly, students possess the experience and knowledge of building risk assessment reports on sectoral, national and global levels. They have the expertise to identify AML failures within financial institutions and provide recommendations to effectively address weaknesses and manage inherent risks. As a result, graduates are well-suited to be employed in various units of the AML risk governance and management structures within organizations.

Finally, students will be exposed to the latest tools and techniques used in financial crime investigations through internships and real-life joint research projects. Their theoretical understanding, combined with practical exposure, enables them to approach financial crime challenges with innovative and effective strategies tailored to the needs of the organization.

Overall, a graduating student with a financial crime degree brings a wealth of knowledge, practical experience and problem-solving abilities that are vital in combating financial crimes and safeguarding organizations from illicit activities. Their contributions can help organizations stay ahead in the ever-evolving landscape of financial crime prevention and detection.

**APC:** *What do you think makes an effective AML professional?*

**MT:** An effective AML professional possesses several key qualities and practices that contribute to their success in combating financial crimes. Based on my experiences and observations, here are some essential aspects of being an effective AML professional:

**Awareness of evolving situations:** AML professionals should stay informed about the ever-changing landscape of financial crimes in their jurisdiction and globally.

**Open-minded observation:** Being attentive and observant with an open mind is critical to the AML process to ensure that all data points, including outliers, are investigated fully.

**Alignment with superior’s agenda:** Understanding and aligning with the priorities and objectives of one’s superiors is essential for effective coordination and teamwork within the organization.

**Straightforward thinking:** AML professionals should adopt a direct and practical approach to problem-solving.

**Proactive updates:** AML professionals should keep superiors and teammates updated with relevant information without being prompted.

**Informal communication channels:** Developing informal communication channels with stakeholders, both within and outside the organization, facilitates effective information sharing and collaboration.

**APC:** *In view of the current state of financial crime in our country, tell us how the AFC community can work better together.*

**MT:** At the national level, it is crucial to establish strong public and private partnerships. But the important question is, where does this begin? If given the opportunity, I would propose an innovative partnership model for the development of an early warning system for financial crime fighters. This system would provide real-time insights into inherent risks associated with specific locations, down to the level of zip codes. Armed with such information, anti-financial crime professionals can proactively address potential threats, preventing criminals from staying one step ahead. **AT**

*ACAMS Pittsburg Chapter board*

SOCIAL MEDIA

# Key AFC updates

Stay ahead with  
*ACAMS Today* on  
LinkedIn and X

