ACAMS TODAY™

ANNUAL CONFERENCE EDITION

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

FILTERING HIGH-RISK CUSTOMERS

NO TECHNOLOGY REQUIRED

ALSO IN THIS ISSUE:

COMBATING TWO EVILS WITH THE SAME TOOLS

VOL. 19 NO. 4 | SEPTEMBER–NOVEMBER 2020
A publication of ACAMS®
acams.org | acamstoday.org

ACAMS TODAY

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

DIRECTOR OF EDITORIAL CONTENT
Kieran Beer, CAMS

EDITOR-IN-CHIEF
Karla Monterrosa-Yancey, CAMS

EDITORIAL AND DESIGN

ASSOCIATE EDITOR:
Stephanie Trejos, CAMS

EDITORIAL ASSISTANT:
Julia del Rivero

INTERNATIONAL EDITOR:
Monica Mendez

CREATIVE AND DESIGN:
Victoria Racine
Joya Jones

EDITORIAL COMMITTEE

CHAIR: Elaine Rudolph-Carter, CAMS
Kevin Anderson, CAMS
Kevin Antis, CAMS
Brian Arrington, CAMS
Edwin (Ed) Beemer, CAMS-FCI
Robert Goldfinger, CAMS
Jennifer Hanley-Giersch, CAMS
Debbie Hitzeroth, CAMS-FCI
Stacey Ivie
Sanjeev Menon
Eric Sohn, CAMS
Joe Soniat, CAMS-FCI
Amy Wotapka, CAMS

SENIOR LEADERSHIP TEAM

INTERIM PRESIDENT:
Angela Salter, CAMS

GLOBAL OPERATIONS & FINANCE:
Sally Helm

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

SENIOR DIRECTOR COMMUNCIATIONS:
Lashvinder Kaur

GLOBAL HR DIRECTOR:
Diana Perez-Saavedra

CHIEF ANALYST/DIRECTOR OF EDITORIAL CONTENT:
Kieran Beer, CAMS

SENIOR MANAGERS

DIRECTOR OF GLOBAL CERTIFICATION AND TRAINING:
Steve Oxman, CAMS

DIRECTOR OF MARKETING:
Fernando Beozzo Salomao

HEAD OF GLOBAL SANCTIONS AND RISK:
Justine Walker

ADVISORY BOARD

CO-CHAIR: Rick A. Small, CAMS
CO-CHAIR: Markus Schulz
John J. Byrne, CAMS
Sharon Campbell
Jim Candelmo, CAMS
Vasilios P. Chrisos, CAMS
David Clark, CAMS, CGSS
Howard Fields, CAMS
María de L. Jiménez, CAMS, CGSS
Lauren Kohr, CAMS-FCI
William D. Langford, CAMS
Dennis M. Lormel, CAMS
Rick McDonell, CAMS
Karim A. Rajwani, CAMS
Anthony L. Rodriguez, CAMS, CPA
John Smith
Daniel D. Soto, CAMS
Dan Stipano
Philippe Vollot

SALES AND REGIONAL REPRESENTATIVES

VICE PRESIDENT GLOBAL SALES
David Karl

SENIOR V.P. BUSINESS DEVELOPMENT:
Geoffrey Chunowitz, CAMS

DIRECTORS OF SALES AMERICAS, CANADA AND LATIN AMERICA:
Sonia Leon, CAMS-Audit
Gerald Sandt

DIRECTOR OF STRATEGIC ACCOUNTS:
Jose Victor Lewis, CAMS

DIRECTOR OF SALES EUROPE:
Paolo Munari

DIRECTOR OF SALES MIDDLE EAST & AFRICA:
Michel Nassif

HEAD OF CARIBBEAN:
Denise Perez, CAMS

DIRECTOR OF SPONSORSHIP AND ADVERTISING DEVELOPMENT:
Andrea Winter, CAMS

REGIONAL DIRECTOR OF BUSINESS DEVELOPMENT - AUSTRALIA:
Nick Griffith

REGIONAL DIRECTOR OF BUSINESS DEVELOPMENT - SOUTH/SE ASIA & JAPAN:
Christine Lim

REGIONAL DIRECTOR OF BUSINESS DEVELOPMENT - NORTH ASIA:
Yokel Yeung, CAMS

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 – GLOBAL HEADQUARTERS
500 W. Monroe, Suite 28
Chicago, IL 60661
USA

Phone: 1-305-373-0020/
1-866-256-8270
Fax 1-305-373-7788
Email: info@acams.org

Websites:
www.ACAMS.org
www.ACAMSToday.org

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

ACAMS

CONTENTS

ON THE COVER:

IN THIS ISSUE

ASPECTS OF APAC

STAFF NOTES

KNOW YOUR CHAPTER

A FILTERING PROCESS

In a podcast I was listening to the other day the presenters were discussing social media. They agreed that when they look at social media they feel as if they need to always do more to keep up with everyone else. To state the obvious, social media has power. While I was contemplating this discussion, I began thinking about how we all instinctually realize this as we upload to social media. We all present a carefully crafted version of ourselves and our experiences via a cornucopia of tools, especially filters, to enhance ourselves and our pictures. Even when we are live and streaming from our social media platforms, we use filters and lighting to ensure we are being viewed in the "correct" way by our followers and potential followers. The idea of putting our cultivated selves on display and the use of filters really hit home as we were preparing the latest edition of *ACAMS Today*. As I read our lead story, "Filtering high-risk customers—No technology required," a sentence written by the author jumped out from my computer screen (where I currently use a filter to help ease my daily eye strain). The author states:

> "Ask any customer-facing bank associate about a customer and chances are the response will be universal—'They're a good customer.' But even good customers present a certain level of money laundering risk. The art of the AML profession is being able to determine which of those 'good' customers present the highest level of risk to the institution accurately. It all starts with knowing your customer."

The "good customer" mirrors someone posting on social media—they have a carefully prepared persona they present to the financial institution. Part of establishing a strong know your customer (KYC) program involves the financial crime prevention professional's ability to pierce through the filter of their customers and apply their compliance programs' policies to determine which customers pose the highest threat. In other words, a financial crime prevention professional needs to be able to look past customers' "filters" to determine when a high-risk customer is presenting themselves as "a low-risk customer." A strong KYC program will utilize many filters and tools to weed out those high-risk customers from the truly "low-risk" customers.

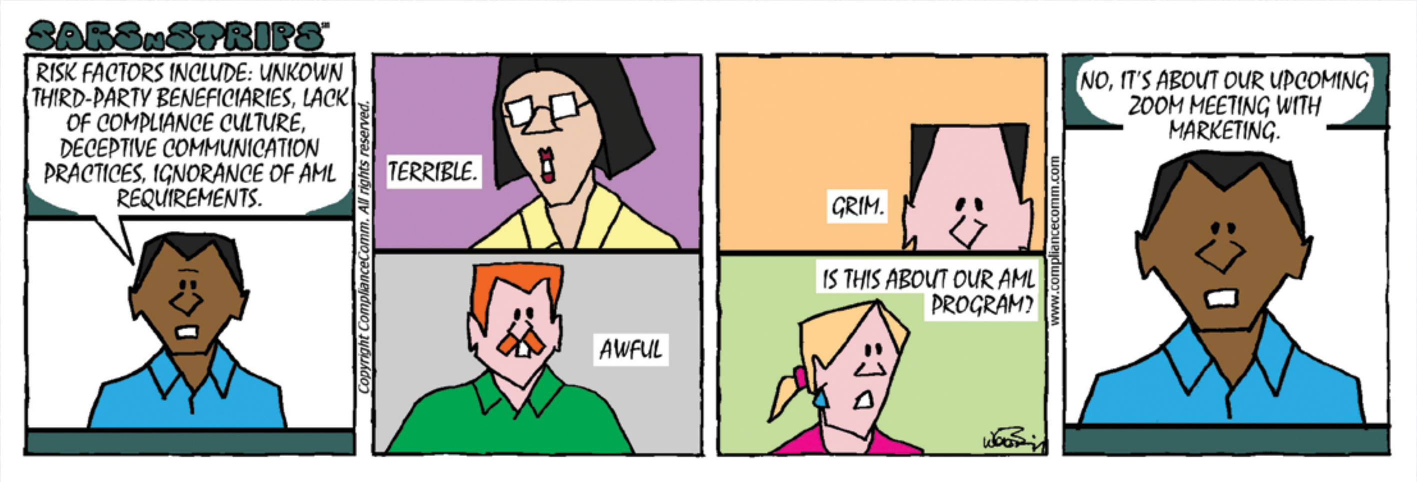
This issue also highlights the diverse challenges facing financial crime prevention professionals, including the second headline article, "Combating two evils with the same tools," which describes how applying counterterrorism laws may help curtail the profitability of human trafficking. Adding to the lineup are articles on the insurance industry, suspicious activity from fund companies, 50 years of the Bank Secrecy Act, a suspicious activity report analysis of the U.K. online gaming sector, potential risks of crypto remittances in the Philippines, illegal wildlife trade and ACAMS chapter events covering topics like COVID-19.

I would like to take this opportunity to congratulate our *ACAMS Today Article of the Year* 2020 recipients. Congratulations to William Cloninger, CAMS; Pawneet Abramowski; Pamela Calaquian, CAMS; Alek El-Kamhawy; William Casey King; Zachary Robock and William Voorhees, CAMS!

Globally, 2020 has presented itself as a challenging year. I hope we will all take the time to filter through the chaos of this year and look for the good in humankind.

Karla Monterrosa-Yancey

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


SARSnSTRIPS
RISK FACTORS INCLUDE: UNKOWN THIRD-PARTY BENEFICIARIES, LACK OF COMPLIANCE CULTURE, DECEPTIVE COMMUNICATION PRACTICES, IGNORANCE OF AML REQUIREMENTS.
Copyright ComplianceComm. All rights reserved.
TERRIBLE.
AWFUL
GRIM.
IS THIS ABOUT OUR AML PROGRAM?
www.compliancecomm.com
NO, IT'S ABOUT OUR UPCOMING ZOOM MEETING WITH MARKETING.

Armina Antoniou, CAMS
Sydney, Australia

Armina Antoniou has approximately 20 years of experience as a risk and legal professional with a broad cross section of Australian and global companies. Antoniou is the general manager of financial crime risk at Tabcorp, Australia's biggest listed gambling and entertainment company and one of the biggest gambling companies in the world. Antoniou leads a team of financial crime specialists who oversee Tabcorp's anti-money laundering/counter-terrorist financing (AML/CTF) and sanctions compliance programs. She supervises Tabcorp's engagement with law enforcement and the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia's financial intelligence unit and AML/CTF regulator. This includes, within AUSTRAC's public-private partnership, engagement with the Fintel Alliance. Antoniou has led and sponsored the financial crime work programs across multiple integration programs at Tabcorp to ensure standardized training as well as operational and systems-based compliance procedures across more than 4,400 retail bet-selling outlets and Australia's largest online betting operator.

Antoniou's previous experience was as a senior lawyer, spending most of her legal career working at one of Australia's and the world's largest law firms, Herbert Smith Freehills. As a seasoned litigator, she appeared in trials before regulatory body investigations and anti-corruption commissions and also participated in significant commercial litigation cases in Australia's federal courts.

Antoniou is also one of Tabcorp's Inclusion Ambassadors, a soccer mum and big sports fan.

Bryan Chapman, CAMS
Pittsburgh, PA, United States

Bryan Chapman has eight years of anti-money laundering (AML) experience, including experience in compliance, fraud and risk mitigation. Currently, Chapman is a detection and investigations manager in the AML operations and financial intelligence unit for PNC Bank. Chapman is a forward-thinking manager of a team of industry-leading investigators responsible for identifying emerging trends, streamlining investigations operations, completing holistic reviews of banking relationships and regulatory filings. Chapman is a subject-matter expert (SME) for cases involving investments, virtual currency, peer-to-peer payments, human trafficking, fraud, trade-based money laundering and COVID-19 scams. This expertise has led Chapman to be a point of contact with several service partners within his own organization, where he is a companywide mentor for the professional development of individuals across different lines of business.

Chapman is currently co-chair for the ACAMS Pittsburgh Chapter. In 2017, he had the exciting opportunity to join a diverse group of SMEs in the AML field in founding the Pittsburgh Chapter. Since joining the chapter, Chapman has presented on various AML investigations involving virtual currency and human trafficking. In addition, he was a panelist speaker on a career development panel for university students that dealt with AML, fraud and cybercrime typologies.

Prior to joining PNC, Chapman worked to prevent insurance fraud with Progressive Insurance, then at the Bank of New York Mellon in roles involving risk, compliance and ethics. He holds a bachelor's degree in criminal justice from California University of Pennsylvania and a master's degree in criminal justice and public policy from California University of Pennsylvania. Chapman has been an ACAMS member since 2014 and he received his CAMS certification in 2016.

Erik Obermeier, CAMS
Frisco, TX, United States

Erik Obermeier is the head of financial crimes compliance (FCC) advisory at Texas Capital Bancshares. In this role, he drives the strategic objectives of the FCC team and the ongoing assessment, redesign and implementation of a Bank Secrecy Act/anti-money laundering (BSA/AML) program that complements the risk profile of the institution. Prior to joining Texas Capital, Obermeier worked for over a decade as a BSA/AML consultant, including with EY, PwC and Accenture.

Obermeier has over 15 years of professional experience, assisting global and regional financial institutions with program remediations, regulatory responses, development and implementation of target operating models and frameworks, shared services centers, policies, procedures and training. He has also managed multiple anti-money laundering (AML) and sanctions risk assessments, AML investigative lookbacks, know your customer (KYC) remediation and transaction monitoring system implementations.

He has shared his AML knowledge with other professionals by speaking at conferences and writing in trade publications on topics that have included leading strategies for regulatory action response, KYC automation and outsourcing. He is an active ACAMS member and has been a Certified Anti-Money Laundering Specialist (CAMS) since 2009.

ACAMS TODAY
ANNUAL CONFERENCE EDITION
FILTERING HIGH-RISK CUSTOMERS
COMBATING TWO EVILS WITH THE SAME TOOLS

FOR FINANCIAL CRIMINALS, THERE IS NO RECESSION

Even in an economic downturn there are plenty of proceeds from crime to be laundered.

Hard times actually create opportunities for human and drug traffickers, and perpetrators of fraud are emboldened to pitch schemes that promise huge returns or magical cures, playing on the desperation of their marks.

Crime associated with COVID-19—the cause of the current worldwide recession, 191,000 deaths in the U.S. and more than 890,000 deaths globally (as I write)—is well-documented.

According to the Financial Crimes Enforcement Network (FinCEN), criminals have become particularly aggressive online, perpetrating phishing schemes, extortion, business email compromises and fraud.

In the July 30 "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," FinCEN lays out red flags for identifying and interdicting cybercrime, starting with a description of how criminals have exploited the vulnerabilities of the remote working conditions necessitated by the pandemic by hacking virtual environments in order to steal sensitive information, manipulate digital identities and use compromised credentials. (The advisory is one of a number released by FinCEN.[1])

Unusual transactions, especially through newly opened bank accounts, are among nearly two dozen red flags listed by FinCEN in the advisory, alongside the use of personal accounts for commercial purposes, corporate names that slightly vary from those of well-known brands, and payments for medical supplies between firms operating in other industries.

Crimes that exploit COVID-19 include the theft of governmental relief funds, including unemployment benefits and other types of international assistance, as documented by the Financial Action Task Force in its May report, "COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses."[2]

So understandably, pursuing cases against criminals involved in COVID-19-related fraud, particularly those stealing from taxpayer-funded programs like the U.S. coronavirus relief bill intended to alleviate suffering caused by the pandemic, has been a priority for the FBI.

Intelligence from anti-financial crime professionals in financial institutions (FIs) is vital to that effort and sometimes responsible for the initial tip off to law enforcement.

Recently, compliance officers at a small New England bank alerted the FBI to loan requests under the Paycheck Protection Plan (PPP) that sought $540,000 to keep dozens of fictitious workers on equally fictional payrolls. Through an enhanced due diligence review that included a drive-by, BankNewport learned that one of the entities seeking a PPP loan, the Apponaug Restaurant Group LLC, was requesting funds for a derelict restaurant that had ceased operating in November 2018.[3]

Separately, an FI in Virginia alerted the Secret Service to a scheme to get a $320 million payment from a foreign government for what investigators later determined were nonexistent face masks.[4]

Nevertheless, even as regulators call on FIs around the world to be on alert for COVID-19-related financial crime (as well as the "usual" illicit financial activity), the economic fallout of the pandemic has generated talk of tighter budgets.

Yet the consequences of cutting back on compliance and starving anti-financial crime efforts could be devastating and costly to FIs that become the victims of undetected fraud and the target of regulators' ire.

Although admittedly COVID-19 is like nothing any of us have seen in our lifetime, we have been through something similar before and would do well to heed lessons learned.

In 2008, when the U.S. housing market collapsed, driving the world into the deepest economic downturn since the Great Depression, many FIs trimmed compliance budgets and cut staff responsible for fighting financial crime.

Initially, regulators focused on safety and soundness and merely murmured their concern that anti-money laundering (AML) issues were being neglected.

But from 2010 through 2015, regulators in the U.S. found reasons to demand hundreds of millions to settle AML violations and even occasional billions—$9 billion, $2 billion (2014) and $1.9 billion (2012).

Beyond monetary penalties, regulators speaking at ACAMS conferences more than once admonished FIs for failing examinations and the costly lookbacks and independent monitors that were the direct result of cutting staffing and resources so severely during the global recession.

Chief executives, general counsels and senior anti-financial crime professionals at banks and other FIs are encouraged to recall this history, however difficult the economic times ahead become.

Compliance departments will need technology, training and staffing to protect their institutions from fraud and to provide law enforcement with invaluable intelligence.

Certainly, financial criminals do not cut back on their efforts during hard times.

Kieran S Beer

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

[1] "Coronavirus Updates," *Financial Crimes Enforcement Network*, https://www.fincen.gov/coronavirus

[2] "COVID-19-related Money Laundering and Terrorist Financing: Risk and Policy Responses," *Financial Action Task Force*, May 2020, https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

[3] Daniel Bethencourt, "FBI Investigating Banker, Convicted Money Launderer and Others Who Sought COVID-19 Loans" *ACAMS moneylaundering.com*, May 12, 2020, https://www.moneylaundering.com/news/fbi-investigating-banker-convicted-money-launderer-and-others-who-sought-covid-19-loans/

[4] Valentina Pasquali, "FinCEN Lists Red Flags for COVID-19 Fraud and Cybercrime," *ACAMS moneylaundering.com*, May 19, 2020, https://www.moneylaundering.com/news/fincen-lists-red-flags-for-covid-19-fraud-and-cybercrime/

QUIZ

Test your AML/CTF knowledge today! Visit ACAMSToday.org to take the latest quiz

1. Which of the following is NOT a category of domestic violent extremism?
a. Racially motivated violent extremism
b. Anti-government/anti-authority extremism
c. Homegrown violent extremism
d. Animal rights/environmental extremism

2. True or false: The Colombian Black Market Peso Exchange was created by criminal organizations to undersell their competition in order to gain market share.
a. True
b. False

3. Which of the following steps should be taken by financial institutions during pandemic (D.P.)?
a. Continue to troubleshoot all technical and operational issues
b. Document and implement strategy to ensure risk-based coverage
c. Identify additional actions based on industry collaboration
d. All of the above

QUIZ

Insured against financial crime

Insurance companies are classified as nonfinancial institutions. Yet in 2002, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) imposed requirements for insurers to comply with the Bank Secrecy Act (BSA), including the responsibility to file suspicious activity reports (SARs) that do not differ much from the ones applied to banks.

The regulation, 31 CFR § 103.137, requires insurance entities that produce or underwrite "covered products"[1] to outline and execute a fully enforceable and applicable written anti-money laundering (AML) program. This program should be aimed at preventing the insurance industry from being used (voluntarily or involuntarily) for money laundering or terrorist financing activities.[2] The following article will cover typologies for money laundering in insurance as well as recommendations for effective risk management.

Money laundering in insurance typologies

FinCEN has disclosed actual instances associating money laundering maneuvers with the insurance sector. In one occasion, a federal law enforcement agency unveiled a narcotics scheme involving cartel bosses in Colombia (Operation Capstone) that were smuggling drug money by acquiring life insurance policies with cash surrender features in offshore geographies. Their illegal (and well-structured) strategy included naming their criminal partners as the beneficiaries and later converting these policies into cash, despite incurring monetary losses when surrendering them. Another case involved the U.S. Customs Service forfeiting proceeds from drug lords that were used to obtain term life insurance policies in Austin, Texas.[3]

Regulators demand rigorous AML compliance from insurance entities because these entities continue to be utilized by money launderers to clean their dirty money. According to FinCEN, approximately 2,500 SARs are filed by insurance companies in a year.[4] One method used by money launderers is buying premium annuities with a single payment instead of making regular premium disbursements over a specific period, especially if the age of the policy beneficiary allows them to obtain access to the funds shortly after they are available to the former policyholder.[5] By doing so, launderers can "wash" their ill-gotten proceeds quickly instead of waiting for several annuity payments throughout the year to attain their final goal.

On other occasions, premium annuities are purchased under a fake name or using a shell company. Then, the annuity is cancelled (regardless of the penalty involved) and the insurance company either sends out a check to the launderer with the remaining balance or wires out the funds to a specific account. The concealed proceeds return as legitimate funds from the insurance company, so they enter the banks clean without generating red flags. Any concerns pertaining to the source of funds are clarified by presenting an insurance contract.[6]

Criminals also launder money by purchasing life insurance policies. In this case, they make additional disbursements, which are later withdrawn in the form of cash surrender value[7] by the policyholder. Cash surrender value is the money the policyowner is entitled to receive from the insurance company upon surrendering a life insurance policy with cash value. Through this method, dirty money enters insurance companies and is later withdrawn as legitimate cash.

Insurance companies allow life insurance premiums be purchased through a third-party loan to cover the cost (also known as premium financing). Thus, money launderers can use illicit money to pay back the loan and receive clean funds from the insurance entity. According to FinCEN, premium financing may not pose high money laundering and terrorist financing risks; however, the arrangements between policyholders and brokers should be scrutinized in detail to avoid potential concealed sources of funds or large atypical cash payments.[8]

Lastly, life insurance policies may also be used by money launderers to borrow against their cash value through "leveraging," or purchasing other financial instruments (such as virtual currency). These investments may be a single gear within a complex illegal money laundering framework (e.g., the usage of structured monetary instruments, trade finance laundering, shell companies and trusts, dummy corporations and nominees).

Recommendations for effective risk management

The insurance broker is often considered a relevant stakeholder within the first line of defense due to their close relationship with prospective and/or current customers (policyholders)—they make the first approach to the client after all. Thus, it is their responsibility to apply effective customer due diligence (CDD). Insurance brokers are also appointed to outline and build a solid, reliable know your customer (KYC) profile that should include exhaustive scrutiny of key financial aspects of the individual or entity being reviewed, such as source of wealth, source of funds and full identification of the ultimate beneficial owner of the policy. Some of the main red flags to look for when performing CDD and KYC processes and when identifying the ultimate beneficial owner are listed below:

- "Customers that are legal entities whose structure makes it difficult to identify the ultimate beneficial owner or controlling interests. (Note: This can happen at inception or, subsequently, an individually owned insurance policy can be assigned to a legal entity. KYC/CDD processes should be applied at both stages.)
- Policy holder and/or the beneficiary of the contract are companies whose structure makes it difficult to identify the beneficial owner, e.g., they are multi-layered or the entity's ownership structure crosses jurisdictions;
- Policy holder and/or the beneficiary of the contract are companies with nominee shareholders and/or shares in bearer form;
- Occupation with a low average income and the policy has high ongoing deposits;
- A history within an occupation with a higher risk for ML/TF due to local crime typologies, high access to cash based businesses or international exposure"[9]

In addition, the first line of defense should create a proper customer identification program. This should include a comprehensive record-keeping methodology accrediting the initial operations and identity of the clients for a period of five years.

Despite the efforts deployed by the first line of defense, the second line of defense (which in this case is compliance) should develop a system to monitor and analyze historical customer behavior that is targeted to look at early policy cancellations (despite the penalties involved). For example, there should be a well-calibrated case management system aimed at capturing atypical operations and transactions on an ongoing basis.

> The first line of defense should create a proper customer identification program

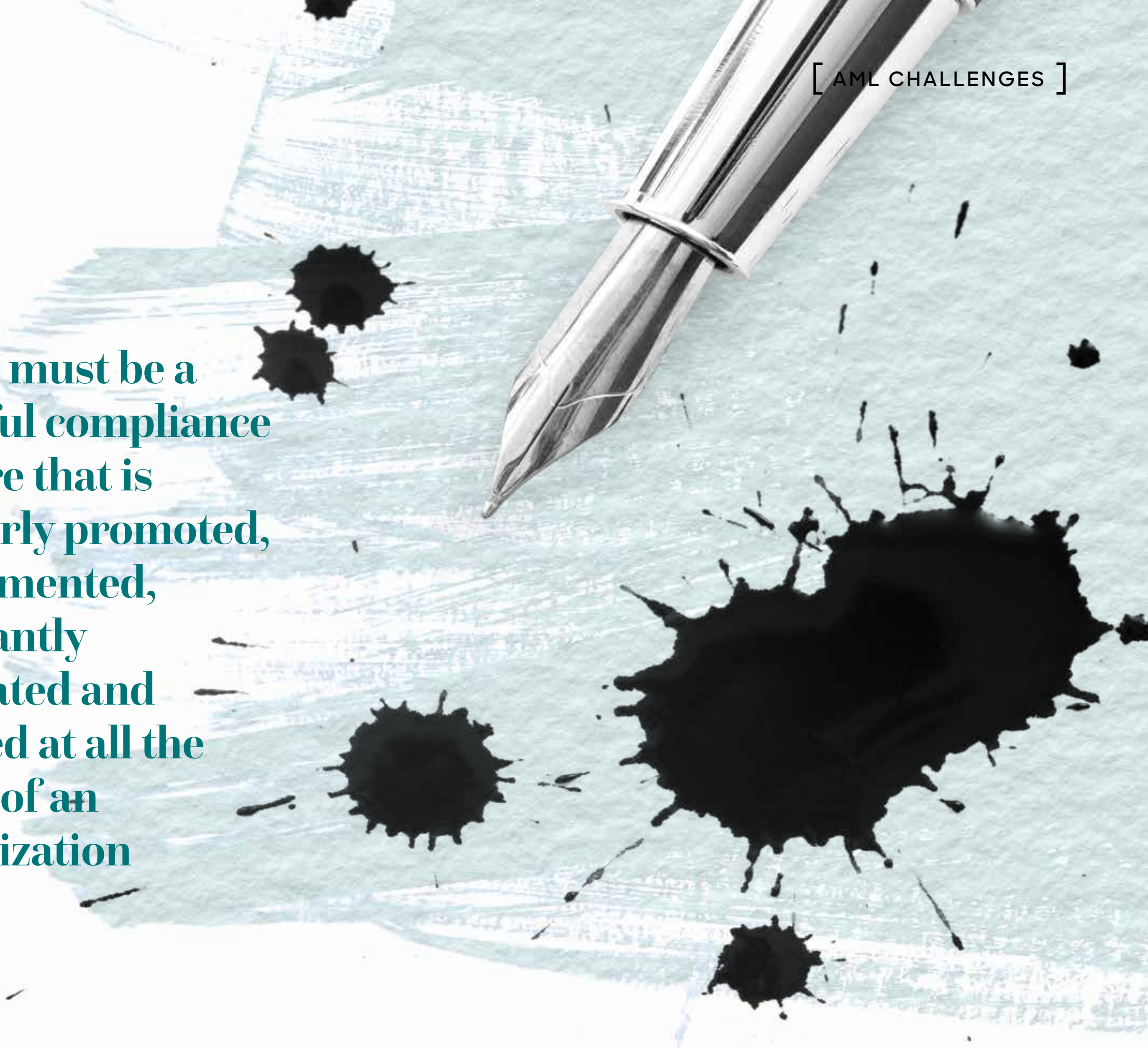
In addition to the CDD carried out by the first line of defense, it is recommended that the second line of defense also conduct enhanced due diligence to rule out any risks that may be associated with possible politically exposed persons and/or derogatory news linked to potential or current policyholders. It is also important to design a realistic risk and control self-assessment aimed at reflecting any potential gaps and ineffectiveness across current internal controls originally implemented to obtain optimal residual risk levels. Insurance companies should also utilize independent reviewers (internal audit) as their third line of defense. The internal auditors should review how applicable and effective the policies, procedures and internal controls are from an unbiased standpoint.

Conclusion

Insurance is another industry that faces money laundering and terrorist financing risks. Lawbreakers are always looking for vehicles to hide the illicit origin of their funds, and individuals linked to terrorist organizations are always seeking ways to funnel and conceal funds that are later used to finance terrorist activities.

Since 2014, FinCEN has received over 15,300 SAR filings submitted by the insurance industry at a steady average of 2,500 per year, potentially indicating that certain criminal organizations still use insurance companies as their preferred means to launder money despite the current stringent BSA regulations that govern that sector.[10]

Insurance products and transactions provide dangerous money laundering and terrorist financing opportunities to criminals. Therefore, there must be a forceful compliance culture that is properly promoted, implemented, constantly evaluated and applied at all the levels of an organization. There must also be strong and effective policies and procedures as well as internal controls, including extensive KYC and CDD best practices across the three lines of defense.



There must be a forceful compliance culture that is properly promoted, implemented, constantly evaluated and applied at all the levels of an organization

Jaime A. Verastegui, MBA, CAMS, CFE, vice president QA compliance manager at a global financial institution, jverastegui44@webster.edu

[1] Per 31 C.F.R. § 103.137, the interpretation behind "covered products" includes a permanent life insurance policy, other than a group life insurance policy; an annuity contract, other than a group annuity contract (or charitable gift annuity); and any other insurance product with attributes of cash value or investment. FinCEN has accepted inquiries concerning the scope of "any other insurance product with features of cash value or investment" and whether group policies or group annuities that authorize individual investments or have cash value for an individual will be considered covered products.

[2] Miriam F. Weismann, *Money Laundering: Legislation, Regulation, and Enforcement* (Chicago: American Bar Association, 2015) 216.

[3] "Anti-Money Laundering Programs for Insurance Companies," *Federal Register*, September 26, 2002, https://www.govinfo.gov/content/pkg/FR-2002-09-26/pdf/02-24144.pdf

[4] "SAR Filings By Industry," *Financial Crimes Enforcement Network*, https://www.fincen.gov/Reports/sar-stats/sar-filings-industry

[5] "Money Laundering in the Insurance Industry," *Asia Insurance Review*, April 2008, https://www.world-check.com/media/d/content_pressarticle_reference/aisaninsurance_08.pdf

[6] James R. Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators* (Routledge, 1998) 108-109.

[7] Harvey W. Rubin, *Dictionary of Insurance Terms*, (New York: Barron's Educational Series, 2013).

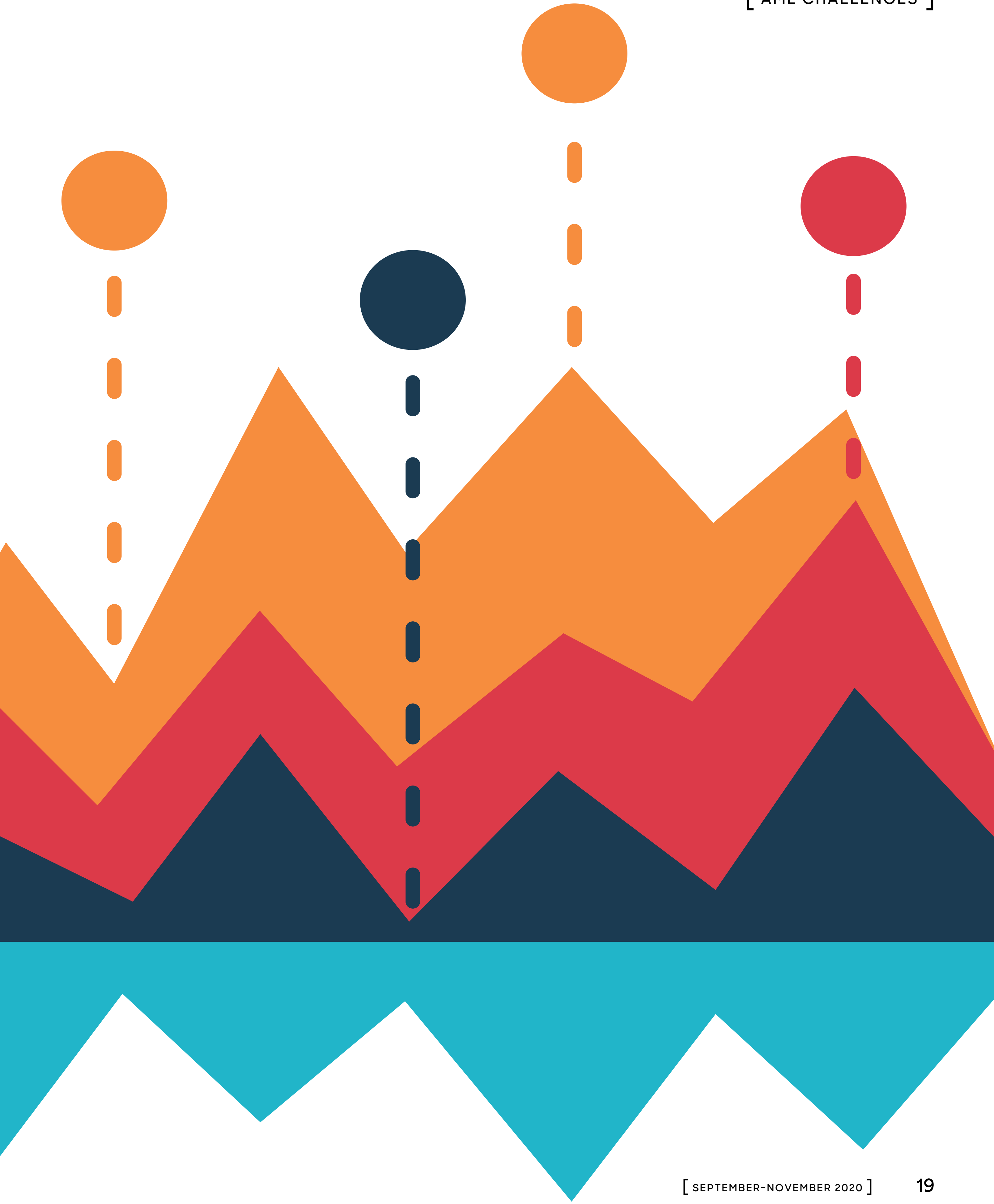
[8] "Interagency Exemption Order," *Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Financial Crimes Enforcement Network*, https://www.federalreserve.gov/supervisionreg/srletters/sr1806a1.pdf

[9] "Guidance for a Risk-Based Approach: Life Insurance Sector," *Financial Action Task Force*, October 2018, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Life-Insurance.pdf

[10] "Anti-Money Laundering Programs for Insurance Companies," *Federal Register*, September 26, 2002, https://www.govinfo.gov/content/pkg/FR-2002-09-26/pdf/02-24144.pdf

Trends in fund companies' AML programs and SAR filings

Anti-money laundering compliance officers (AMLCOs) often observe situations where their clients or partners may struggle with deciding whether to report suspicious activity in accounts where no suspect can be identified. Based on recent regulatory filings, there appears to be an increase in suspicious activity detection and reporting by financial institutions (FIs), even in instances where the suspicious activity detected falls short of reporting requirements. Such voluntary reporting provides law enforcement, regulators and the industry more robust information that may be leveraged to enhance anti-money laundering (AML) and financial crime prevention. This article will explore the reporting requirements imposed on investment companies and discuss what conclusions can be reached about trends in reporting suspicious activity.



Background

In May 2006, the Financial Crimes Enforcement Network (FinCEN) published in the Federal Register[1] its final rule requiring mutual funds to file reports that identify and describe transactions that suggest suspicious or illegal activity in the securities and futures industries on FinCEN Form 101 (SAR-SF). Mutual funds are required to report the following to FinCEN:

- Any transaction conducted or attempted by, at or through a mutual fund that, alone or in the aggregate, involves at least $5,000 in funds or other assets, if the mutual fund knows, suspects or has reason to suspect that the transaction involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity
- Any transaction that is designed, whether through structuring or other means, to evade BSA requirements
- Any transaction that has no business (including investment) or other apparent lawful purpose or is not the sort of transaction in which the particular customer would be expected to engage, and for which the mutual fund knows of no reasonable explanation after examining the available facts, including the background and possible purpose of the transaction
- Any transaction that involves the use of the mutual fund to facilitate criminal activity, including those transactions in which legally derived funds are used for criminal activity[2]

Mutual funds typically conduct operations through separate entities, which may or may not be an affiliated person of the mutual fund, such as investment advisers, principal underwriters, administrators, custodians and transfer agents (service providers). According to FinCEN,

> "A mutual fund may contract with an affiliated or unaffiliated service provider to perform the reporting obligations as the fund's agent. However, the mutual fund remains responsible for assuring compliance with the regulation and must monitor performance by the service provider. The mutual fund should take steps to assure itself that the service provider has implemented effective compliance policies and procedures administered by competent personnel, and also maintain an active working relationship with the service provider's compliance personnel."[3]

On January 7, 2020, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) announced its 2020 examination priorities. The OCIE will continue to review for compliance with applicable AML requirements, including whether entities are appropriately adapting their AML programs to address their regulatory obligations.[4]

For the purposes of this discussion, several service providers and other representatives in the financial industry were interviewed, specifically 10 AML compliance officers of transfer agents (TA AMLCOs), to determine whether they observed an increase in suspicious activity from May 2018 to April 2020. For those TA AMLCOs who had perceived an increase in suspicious activity, the scope of the analysis was narrowed to SAR filings in securities and futures industries (SAR-SF) and the following questions were presented:

- How was the suspicious activity detected (e.g., automated reports)?
- What type of suspicious activity was detected (e.g., identity theft)?
- What was the methodology utilized to notify the AMLCO of the mutual fund (fund AMLCO)?
- Did the TA AMLCO file the SAR-SF or did the fund AMLCO file the SAR-SF?
- What was the verification process of the suspect's identity? Was the suspect known or unknown?

Increase in suspicious activity reporting

All TA AMLCOs interviewed detected an increase in suspicious activity over the past two years, as further evidenced by FinCEN SAR data. SAR Stats (formerly The SAR Activity Review by the Numbers), which is a compilation of numerical data gathered from FinCEN SARs, is publicly available. According to this data, suspicious activity has increased by 39% in just two years (refer to Exhibit 1 below).

Exhibit 1:

SAR-SFs filings by year[5]

Year	SAR-SFs filings by year	Rate of increase
2017	23,832	-
2018	26,776	12%
2019	33,222	24%

Detection of suspicious activity

In most cases, suspicious activity was detected by monitoring daily reports generated by advanced analytics, monitoring software and artificial intelligence. The activity flagged in these reports included pattern activity, accounts opened online, deficiencies identified during the new account process, insufficient funds, use of unauthorized funds, internal red flags process and shareholder concerns. The average TA AMLCO monitors approximately 10 automated reports daily.

Types of suspicious activity detected

FinCEN SAR data, as supported by the TA AMLCOs interviewed, indicated that the top activities reported on SAR-SFs were wire fraud, identity theft, and anomalies in automated clearing house (ACH) payments (refer to Exhibit 2 below).

Exhibit 2:

Number of SAR-SF filings by type of suspicious activity[6]

Rank	Suspicious activity type	Filings (overall)
1	Wire fraud	33,709
2	Identity theft	32,597
3	ACH	25,176

Notification to fund AMLCO

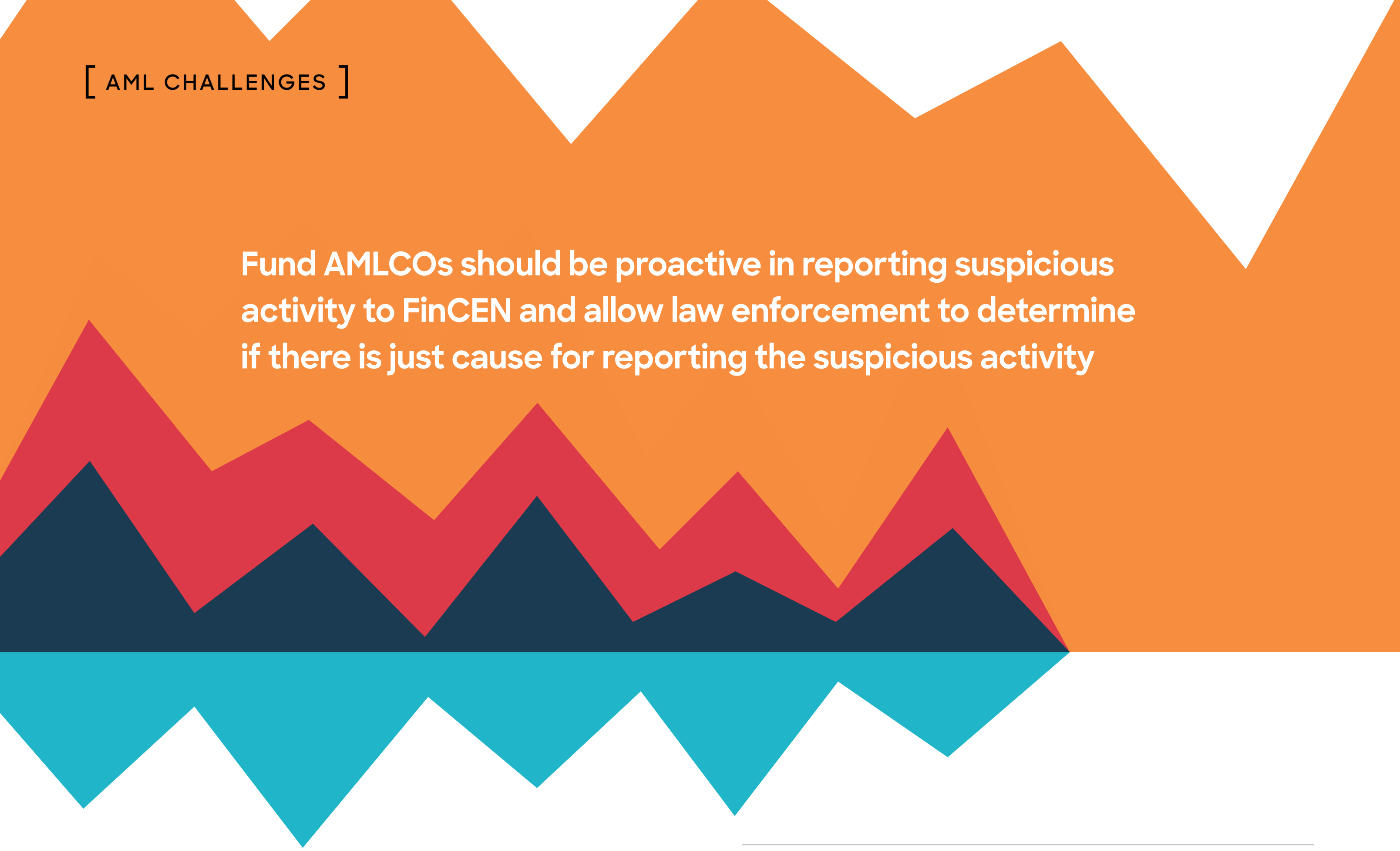
Typically, once a TA AMLCO detects unusual activity and determines it is reportable activity, a narrative is emailed to the fund AMLCO for record retention purposes. If a determination is made by either party that filing a SAR-SF is required or appropriate, the TA AMLCO would prepare and file the SAR-SF in most instances. It should be noted here that there may be circumstances where one FI that has detected the suspicious activity may have an independent obligation to report suspicious transactions, despite a fund AMLCO's determination not to file. For example, the transfer agent may have detected patterns of transactions—such as a new client opening an account online and using false identification—and may have more information at its disposal to identify the need to file a SAR-SF or to explain why a SAR-SF is not required.

As required by FinCEN, "mutual funds are encouraged to report voluntarily transactions that appear relevant to violation of law or regulation, even in cases in which the rule does not explicitly require filing of a Suspicious Activity Report–such as transactions that, alone or in the aggregate, fall below the $5,000 threshold." Furthermore, mutual funds are required to report suspicious activity if the transaction meets the "knows, suspects, or has a reason to suspect (or patterns of transactions)" standard.

The SAR-SF filing process

Since April 1, 2013, FIs must use the BSA E-Filing System[7] in order to submit a SAR-SF under FinCEN Report Form 111. The SAR-SF is divided into five sections: subject information, suspicious activity information, information about the FI where the activity occurred, filing institution contact information and a narrative that enables the reader (investigators, regulators, etc.) to identify trends of fraudulent activity within the industry. Emphasis on the "who, what, where, when, why and how" will provide a thorough description of the activity and the basis for filing the SAR-SF. After the SAR-SF is submitted, the system will generate a confirmation for record retention purposes and the TA AMLCO will provide a copy of the confirmation to the fund AMLCO.

Mutual funds are required to report suspicious activity if the transaction meets the "knows, suspects, or has a reason to suspect (or patterns of transactions)" standard



Fund AMLCOs should be proactive in reporting suspicious activity to FinCEN and allow law enforcement to determine if there is just cause for reporting the suspicious activity

The background section indicates that one of the minimum requirements is violations aggregating $5,000 or more where a suspect can be identified. In recent years, it has become a best practice to file a SAR-SF when the identification of the suspect has not been verified, primarily because the details relating to suspicious activity may be useful to law enforcement. Not only is this used in following up on specific criminal investigations, it is also used by others in law enforcement, such as SAR review task forces, in identifying trends, patterns and typologies of fraudulent activity. For example, detected suspicious activity may be related to a particular IP address configuration, which may be helpful in determining the location where the suspicious activity originated, even though an individual could not be identified. This particular information could help a specific investigation or be part of a pattern that could be useful in future investigations.

Conclusion

As evidenced by the information obtained from service providers and other representatives in the financial industry—specifically the TA AMLCOs interviewed—and substantiated by FinCEN's SAR Stats, there does appear to be an upward trend in suspicious activity detection and reporting. Although the information may not meet the minimum requirements for filing a SAR-SF, all the information provided on a SAR, especially a comprehensive narrative, is useful. Only law enforcement prosecutes, but regulators, including the SEC, and the industry have duties to help detect and prevent money laundering as well as other financial crimes. Therefore, fund AMLCOs should be proactive in reporting suspicious activity to FinCEN and allow law enforcement to determine if there is just cause for reporting the suspicious activity.

Nancy J. Tyminski, director, Foreside Financial Group, Berwyn, PA, USA, ntyminski@foreside.com

[1] "Financial Crimes Enforcement Network; Amendment of the Bank Secrecy Act Regulations-Requirement That Mutual Funds Report Suspicious Transactions," *Federal Register*, May 4, 2006, https://www.federalregister.gov/documents/2006/05/04/06-4177/financial-crimes-enforcement-network-amendment-to-the-bank-secrecy-act-regulations-requirement-that

[2] "Frequently Asked Questions Suspicious Activity Reporting Requirements for Mutual Funds," *Financial Crimes Enforcement Network*, October 4, 2006, https://www.fincen.gov/index.php/resources/statutes-regulations/guidance/frequently-asked-questions-suspicious-activity-reporting

[3] "Financial Crimes Enforcement Network; Amendment of the Bank Secrecy Act Regulations-Requirement That Mutual Funds Report Suspicious Transactions," *Federal Register*, May 4, 2006, https://www.federalregister.gov/documents/2006/05/04/06-4177/financial-crimes-enforcement-network-amendment-to-the-bank-secrecy-act-regulations-requirement-that

[4] "SEC Office of Compliance Inspections and Examinations Announces 2020 Examination Priorities," *U.S. Securities and Exchange Commission*, January 7, 2020, https://www.sec.gov/news/press-release/2020-4

[5] Statistics generated for this report were based on the BSA Identification Number (BSA ID) of each record within the SAR-SF system. The BSA ID is a unique number assigned to each SAR-SF submitted. Numeric discrepancies between the total number of filings and the combined number of filings of states and/or territories are a result of multiple locations listed on one or more SAR-SFs.

[6] Some SAR-SF filings may list multiple suspicious activities. The date range includes January 1, 2014, through December 31, 2019.

[7] *BSA-E Filing System*, https://bsaefiling.fincen.treas.gov

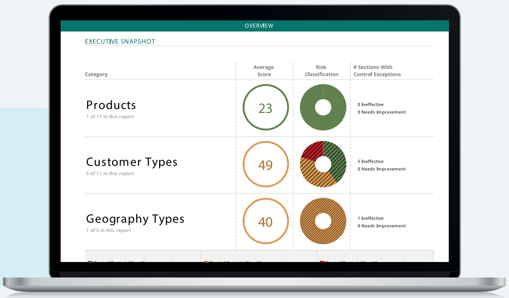
ACAMS RISK ASSESSMENT™

MEASURE, UNDERSTAND AND EXPLAIN YOUR MONEY LAUNDERING RISKS

Based on a methodology designed and consistently optimized by public and private sector AML experts, ACAMS Risk Assessment is a web-based solution that delivers a comprehensive, automated risk-based profile of an institution's products, services, geographies and customer entities through a flexible and scalable platform for institutions of all sizes.

www.acamsriskassessment.com

Email us to schedule a demo at:
riskassessment@acams.org



OVERVIEW

EXECUTIVE SNAPSHOT

Category	Average Score	Risk Classification	# Sections With Control Exceptions
Products 1 of 17 in this report	23		0 Ineffective 0 Needs Improvement
Customer Types 5 of 11 in this report	49		5 Ineffective 0 Needs Improvement
Geography Types 1 of 5 in this report	40		1 Ineffective 0 Needs Improvement

ACAMS

A practical approach to PEP risk management

A good PEP today can turn into a bad PEP tomorrow

Managing risk associated with politically exposed persons (PEPs) is increasingly becoming an area of focus among financial institutions (FIs) around the world. This increase is due not only to changing regulatory requirements, but also to headlines that have cast many organizations in an unfavorable light for banking some PEPs.

PEPs can create increased risks and costs if not managed well. However, an effective risk-based approach tailored to one's organization's global risk policies and requirements can greatly alleviate the risks and difficulties of PEP management.

Why PEPs pose challenges for organizations

The elusive nature of PEP risk is what makes properly and efficiently identifying it especially challenging. As a result, organizations tend to cast a wide net on their risk detection, causing high levels of false positives.

PEPs are moving targets

With hundreds of elections taking place each year, a client in an organization's customer base can become a PEP at any given time. Moreover, a good PEP today can turn into a bad PEP tomorrow, as some institutions have learned after having woken up to find that they were serving an account of one of the world's most corrupt actors.

Information is hard to obtain

Obtaining PEP information globally is not as straightforward as one might think, with a varying degree of difficulty by country. Data protection laws can create challenges, with certain countries such as Belgium and Germany not publishing complete information. According to the Fifth AML Directive, European Union member states should have begun providing PEP information in a timely manner as of January 2020, but some have not yet fully obliged.

Different definitions of PEP by jurisdiction

As the Wolfsberg Group's 2017 PEP Guidance states, there is no single, globally agreed upon definition of a PEP. Therefore, it is important to identify which types of PEPs matter to one's organization and to understand the variations of local PEP definitions in the jurisdictions in which one operates.

In the United Kingdom (U.K.), if a person who is a PEP is no longer entrusted with a prominent public function, that person should continue to be subject to risk-based enhanced due diligence for a period of at least 12 months after the date they ceased to be entrusted with that public function.[1] However, the 12-month period does not apply to their relatives and close associates (RCAs). In Canada, "a person determined to be a foreign PEP is forever a foreign PEP,"[2] but a person ceases to be a domestic PEP five years after they have left office, and that extends to their family members and associates as well.

Involvement of agents and middlemen

History shows that in many high-profile PEP-related corruption cases, risk is primarily associated with the middleman and advisors, or a company, trust, charity or similar financial vehicle used to facilitate transactions. In fact, the political figure is usually the last person in the PEP risk train. This highlights the importance of obtaining a full picture of a customer, including their networks and beneficial ownership associations.

Knowing who are the good PEPs and who are the bad PEPs

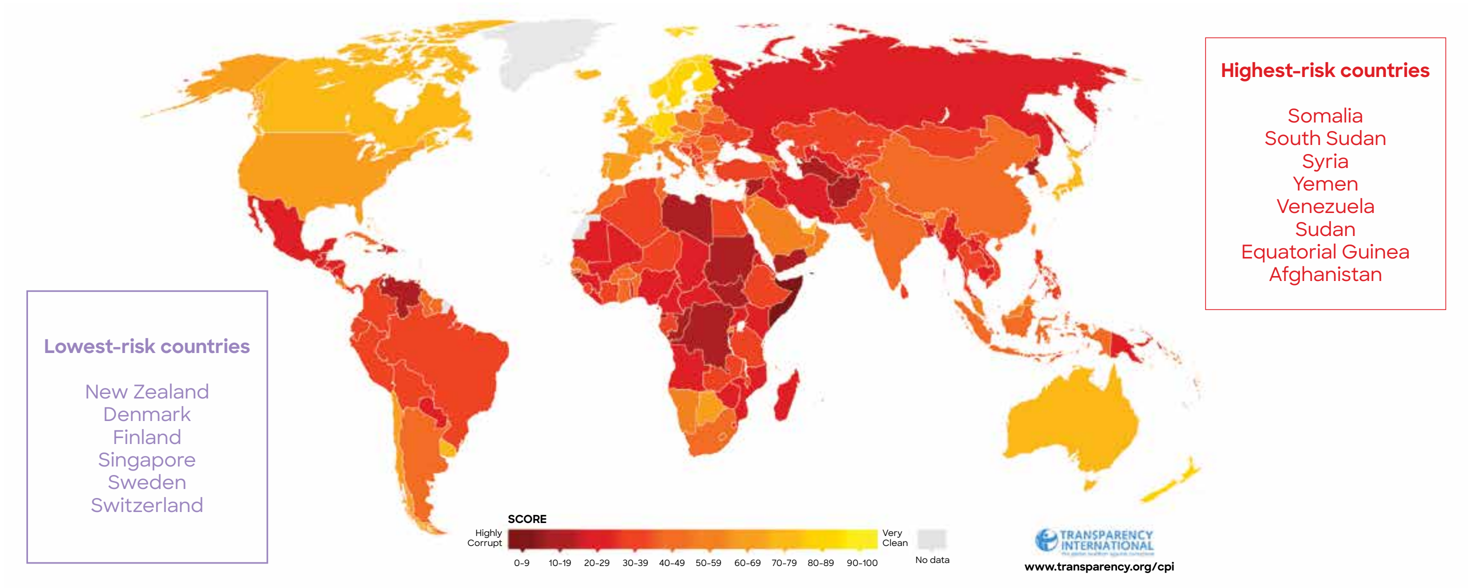
Most PEPs are good people. As the Financial Action Task Force (FATF) says, PEP risk management requirements are preventative in nature and should not be interpreted to stigmatize PEPs as being involved with criminal activity.

However, a corrupt official will go out of their way to conceal their identity and source of wealth. Therefore, effective anti-money laundering (AML) requires an assessment of corruption-related risk and protection against the laundering of corruption proceeds across a spectrum of customers, businesses and business relationships.

PEP risk management is certainly a moving target that creates growing challenges for organizations. "Good guy today, bad guy tomorrow" is the familiar mantra for many a seasoned compliance officer. However, there is a practical and effective approach that can alleviate the burden of managing PEPs.

Figure 1:

Corruption Perceptions Index 2019



Highest-risk countries

Somalia
South Sudan
Syria
Yemen
Venezuela
Sudan
Equatorial Guinea
Afghanistan

Lowest-risk countries

New Zealand
Denmark
Finland
Singapore
Sweden
Switzerland

www.transparency.org/cpi

Developing a practical risk-based approach to PEP challenges

Start with a risk assessment

Developing a risk-based solution to PEP challenges starts with assessing risk factors, such as types of business, product range, partners, subsidiaries, correspondent banks and where one operates. Higher-risk jurisdictions are defined as having significant deficiencies in their AML regimes, so the regulatory expectations and the level of due diligence required in these regions will vary. Figure 1 illustrates some of the highest and lowest risk countries in the world.

PEP types and categories

Managing PEP risk can be both time consuming and expensive, especially if using a “one-size-fits-all” approach. A smarter approach to controlling both risk and productivity involves first understanding what types and categories of PEPs matter to the business and using various filters to identify different types of PEP risk. This means applying a tailored risk-based approach that involves higher scrutiny for certain categories and less for the rest, or even excluding certain categories altogether in a review.

Primary PEPs—individuals who are or have been elected or appointed to a prominent public position—are typically divided into categories based on their level of governance. This allows for selecting specific categories based on a company’s business and risk appetite. For instance, the international organizations category includes members of the United Nations and the World Trade Organization. National governments include heads of state and members of parliament. Subnational governments include regional and local government roles, such as city officials. Nongovernment PEPs include influential religious leaders and political groups, among others. International and national government PEPs are typically considered higher risk, while local and nongovernment roles can be viewed as lower risk. However, each company will apply their own risk-based approach to determine the level of risk associated with each of these categories.

Filtering the PEP categories to align with a risk-based approach and regulator expectations helps reduce downstream review efforts, allowing efficient PEP risk management without increasing risk exposure.

A holistic approach

A holistic but practical way to address the PEP challenge consists of a 3D, risk-based approach (see Figure 2).

In this approach, there are three major elements to consider: the client data, the PEP data and the matching rules used to screen those two sets of data against each other. Having a clear understanding of these three elements and leveraging them to one’s advantage can greatly improve the quality of your matches.

Across both the client and PEP data, conducting a data analysis is a great starting point to help better understand data strengths and weaknesses. These analytics can then be used to configure matching rules for ultimately enhancing the ability to detect risk.

1. *Client data*
   - A data quality analysis or assessment of internal data helps identify any data issues so matching rules can be tailored to accommodate. For instance, if client data has very little date of birth information, this needs to be addressed by allowing for matches with a blank date of birth.
   - A data quality assessment will also identify data issues such as missing surnames, joint accounts, dummy or invalid data entries, and duplicate customer records. If duplicate records can be combined while still keeping the data lineage, alert disposition efforts can be reduced and a proper audit trail can be maintained.
   - The product risk of the client data could also be considered. For example, client data for life insurance policies holds a very different type of risk from client data for car insurance. Depending on the risk profile of the client data, the matching rules can be adjusted.

2. *PEP data*
   - With commercially available global PEP databases containing an average of 1.5 million or more PEP and PEP-related profiles, being able to slice and dice and have granular control over what to screen against or disregard, or when to apply looser or tighter matching rules, is key to reducing false positives. For instance, as part of demonstrating a risk assessment for the business and regulator, one should be able to differentiate between foreign versus domestic PEPs or choose specific countries and combine that filter with certain PEP categories. One should be able to consider certain PEP categories in high-risk countries as high risk, while considering those same PEP categories in low-risk countries as lower risk.
   - Further, if the risk-based approach allows it, one can exclude certain types of PEPs from screening. For instance, low-risk PEP data in certain countries and PEPs that have been out of office for a given amount of time can be excluded. This will have a big impact on the number of PEPs to be screened and, consequently, the number of possible matches generated for review.
   - Just as with the client data, consider the basic quality of the PEP data that is being screened. Since PEP data quality can vary by country and PEP category, it is important to consider this and ensure that the matching criteria is set up accordingly to bring back optimal results.

3. *Matching rules*
   - Matching rules are where the magic happens. The rules are adjusted based on the already completed client and PEP data analysis, combined with the risk requirements and appetite of the organization across different geographies, products, channels, etc.
   - Consider which secondary identifiers are available for screening and ensure they are being used in matching configurations.
   - In addition, it is important to ensure that screening systems are capable of this granular level of matching and filtering to reflect a risk-based approach and keep the false positives to a minimum.

Figure 2:

A 3D risk-based approach

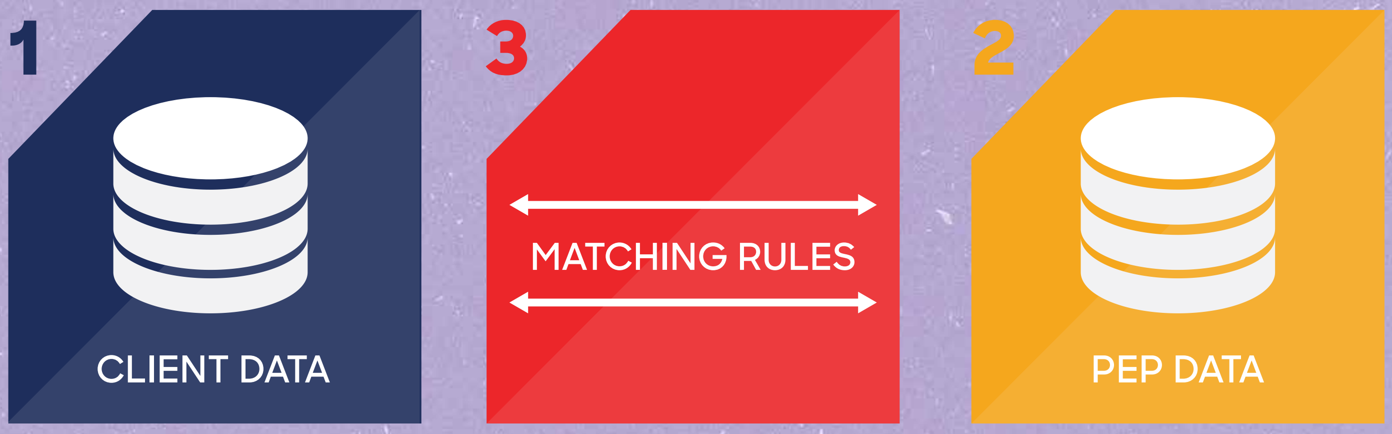
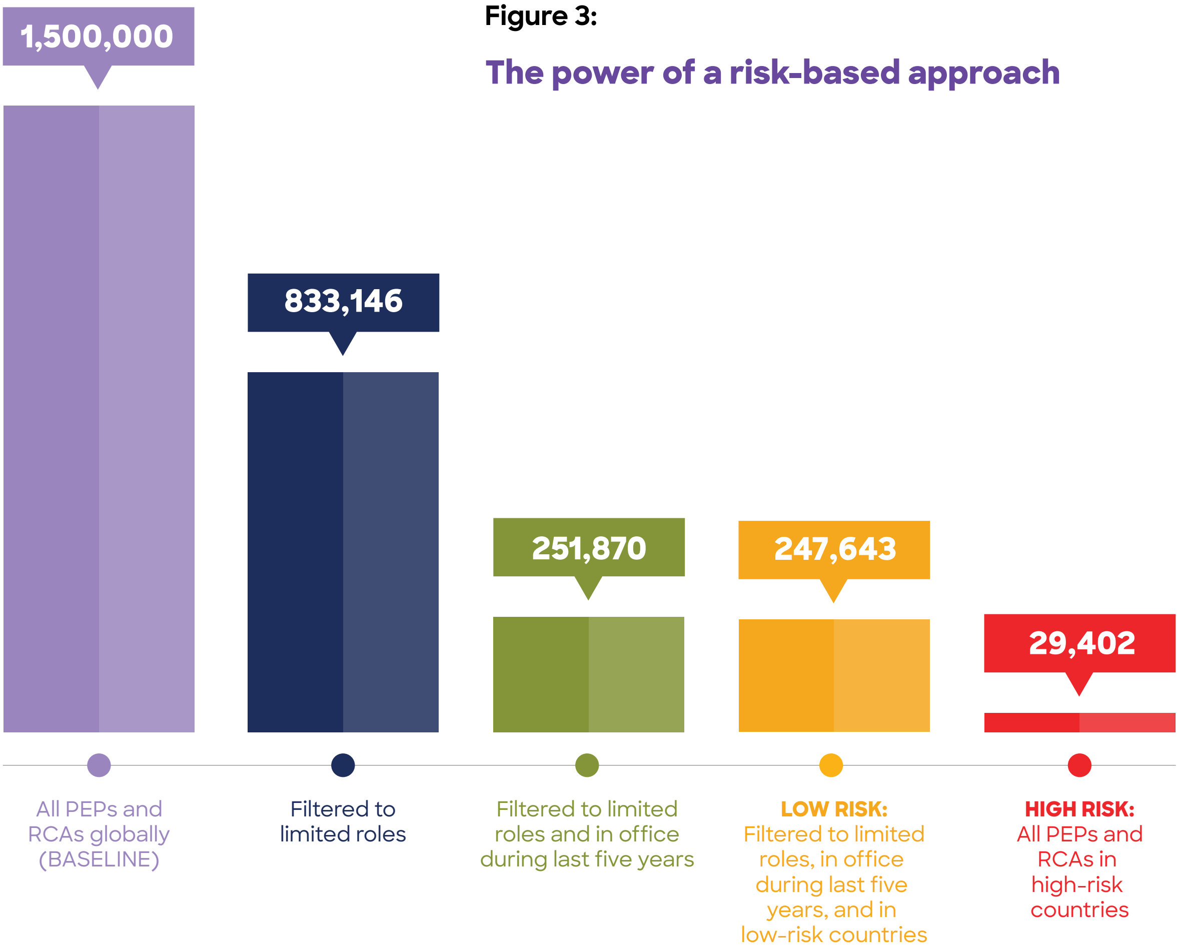


Figure 3:

The power of a risk-based approach



Having granular control over the PEP database within a screening system can have a huge impact on workload.

Filtering out nonrelevant PEPs based on a company's risk-based approach will have a significant impact on productivity, as shown in Figure 3 above.

Summary

A one-size-fits-all approach to PEP risk management can result in unnecessary effort and possibly divert resources from where they are most critically needed.

For more accurate identification of risk while reducing false positives, consider adopting the 3D, risk-based approach that considers internal data, PEP data and matching rules. This provides the ability to achieve efficient monitoring of PEP risk as well as the ability to explain and defend the approach to auditors and regulators.

Neil Marshall, data & screening specialist, FinScan, Pittsburgh, PA, USA, nmarshall@innovativesystems.com

Benjamin Krige, principal consultant, professional services, FinScan, Pittsburgh, PA, USA, bkrige@innovativesystems.com

[1] "FG 17/6 The treatment of politically exposed persons for anti-money laundering purposes," *Financial Conduct Authority*, https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf

[2] "Politically exposed persons and heads of international organizations – Financial entities," *Financial Transactions and Reports Analysis Centre of Canada*, June 2017, https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide12/12-eng

ACAMS™

CGSS™
CERTIFIED
GLOBAL SANCTIONS
SPECIALIST

CERTIFIED GLOBAL SANCTIONS SPECIALIST (CGSS)

An ACAMS certification that equips an organization's workforce with a global credential that represents a serious commitment to compliance with sanctions regulations.

Through September 30, 2020, ACAMS will offer online proctoring for candidates taking their CGSS certification exam via Pearson VUE's online proctoring system, OnVUE.*

Download the Candidate Handbook:
www.acams.org/cgss

*Online proctoring availability is limited and subject to change.

ACAMS

Combating two evils with the same tools

In the midst of uproar and hot-button debates over historical slavery in the U.S., virtually none of the discourse calls attention to the fact that slavery continues around the world in the form of human trafficking. In June 2020, Wilhan Martono was arrested in northern California for allegedly operating a $21 million human trafficking business.[1] While the more heinous aspects of Martono's activities include the trafficking of children, he attempted to cover his tracks through judicious money laundering activities. First, buyers paid in bitcoin or prepaid cards, then funds were layered through wire transfers before finally being integrated into bank accounts and stocks of hard silver bullion.[2] According to a 2019 report by the U.S. Department of State, approximately 25 million people worldwide live in a condition of slavery as the result of human trafficking.[3] For perspective, this is over twice the current populations of Greece or Portugal. Fortunately, the tools of combating one evil are often useful in countering another. In the case of human trafficking, laws against terrorism offer a viable path forward to curtailing its profitability and assisting victims with rebuilding their lives.

While the actual laundering of human trafficking profits, like those of any predicate crime, can be layered through numerous avenues, the ultimate resting place of the resulting wealth is the banking sector. Banks offer a level of efficiency and liquidity that is unavailable when wealth is encapsulated in some other form. Like the case of Martono, most money derived from crime inevitably becomes reintegrated into the financial system by entering a bank. Legislation designed to combat terrorist financing by opening banks to civil liability can be replicated to combat human trafficking.

After 9/11, legislation and regulation was designed to cut off the funding from terrorism proliferated around the world, while civil "lawfare" in U.S. courts empowered victims of terrorism to sue banks or other corporate entities that were involved in terrorist financing. Two laws in particular, the Anti-Terrorism Act (ATA) and the Justice Against Sponsors of Terrorism Act (JASTA), offer clear pathways for victims seeking restitution.

The ATA serves as the basis for several high-profile civil suits in U.S. courts. Over the first two decades of the new millennium, a number of high-profile cases were brought by terror victims and their families against banks Arab Bank, BLOM Bank, National Westminster Bank and Crédit Lyonnais for allegedly facilitating the financing of the Palestinian terrorist group Hamas.[4] It is also worth noting that the ATA's reach goes beyond banks and financial institutions (FIs) to other types of businesses. For example, the families of missionaries in Colombia who were murdered by the Revolutionary Armed Forces of Colombia (FARC), a left-wing drug trafficking organization, filed a federal suit against the fruit company Chiquita Brands International for the company's alleged material support of the terrorist group.[5] Such cases provide an inspiring parallel for potential legislation to incentivize FIs to put controls in place that would make it more difficult for traffickers to integrate their illicit proceeds into the legitimate global economy.

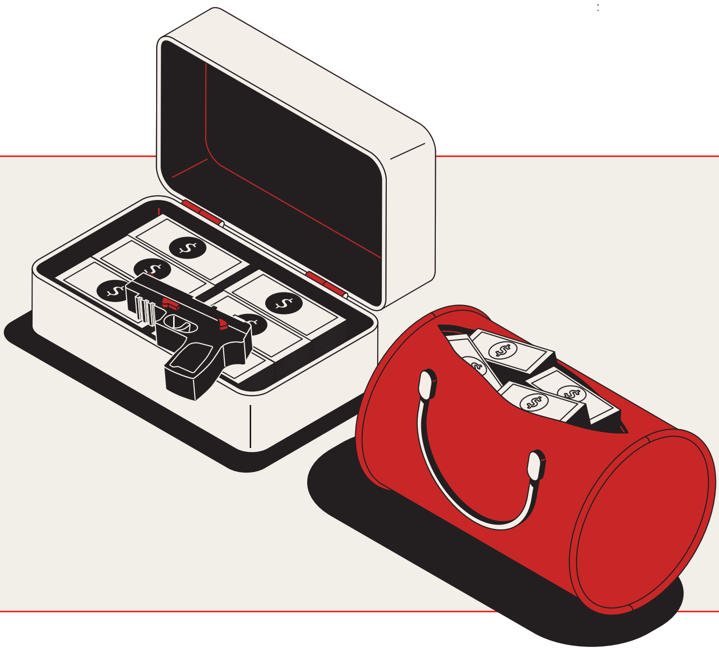
The language of the ATA is very clear in its provision of civil liabilities to economic entities involved in terrorism and in offering a path for victims to obtain monetary compensation. Compared to most statutes designed to combat human trafficking, laws such as the ATA are notably aggressive in enabling victims to seek damages in civil court from third-party entities. Key legislation against human trafficking, such as the Trafficking Victims Protection Act and its subsequent amendments, do not have the same approach as the ATA. The conceptual difference between terrorism and human trafficking is one of the reasons for this dissonance.

Conceptual differences between terrorism and human trafficking

Terrorist financing is similar to money laundering in that both activities seek to distance and obfuscate the origins of funds from their end user. A criminal who is not a terrorist must obfuscate the resulting proceeds from the predicate crime that they committed. Thus, when laundering is added to criminal charges, it provides an additional avenue of prosecution and means by which to secure a conviction. In contrast, terrorist financing may often involve funds that are legally or illegally obtained through the conduct of normal business or fundraising but are destined to support an illegal outcome. Laws designed to combat terrorist financing are meant to prevent terrorism as a future crime. Despite the heinous nature of human trafficking, it is still legislatively treated as a crime that has already occurred rather than one that must be prevented.

Human trafficking carries greater operational costs due to the need to keep victims healthy, fed, and constantly guarded or intimidated

Human trafficking comprises an economic activity and a rather costly one when compared to other illicit trades such as black-market antiquities, drugs or arms dealing. Unlike nonhuman contraband, human trafficking carries greater operational costs due to the need to keep victims healthy, fed, and constantly guarded or intimidated. Such activities are incredibly expensive for traffickers, so one key to curtailing systematic trafficking is to attack its economic viability by raising its cost of business. More complicated and costly operations require more funds, while the use of such funds requires more laundering. Enabling victims to file civil suits against banks and other going concerns involved in their trafficking can be accomplished by passing legislation



Human trafficking is already immoral; however, making it unprofitable and increasing its risk is the key to ending the practice

modeled on the ATA. Such legislation would raise the costs of the human trafficking business, and disincentivize criminals from entering into it.

One key difference between the ATA and U.S. laws to combat human trafficking is that the former makes third parties culpable in the economic activity leading to terrorism, while the latter does not. Sections 108 and 109 of the Justice for Victims of Trafficking Act of 2015 opens "buyers" of trafficking victims to prosecution, but not third parties such as banks or other entities involved in the transaction. A terrorist group can only operate by using third parties such as banks, transportation firms, telecommunications and other businesses that make their activities viable. Similarly, human trafficking on any significant scale must rely on more tertiary actors beyond the dyad of trafficker and buyer.

In the case of Chiquita and the FARC, the company provided the terrorist organization with monthly cash payments[6] and weapons.[7] While federal law through the ATA allows for victims and their families to pursue damages from third parties with a firm legal grounding, the same solid legal basis does not exist for human trafficking victims. Recently, major hotel chains such as Wyndham, Marriott and Hilton became the targets of lawsuits brought by human trafficking victims.[8] Logistically, major hotel chains—especially in locales close to international borders or tourist locations—constitute a critical element of the human trafficking enterprise. The state of Florida passed legislation mandating training for the hospitality industry to assist in spotting trafficking.[9] Such anti-trafficking mandates are similar to the mandatory compliance standards imposed on the financial industry as it pertains to terrorist financing. However, unlike the ATA, third parties are not statutorily culpable for civil liabilities.

Conclusion

Anti-human trafficking groups could easily draw from the ATA and other counter-terrorist financing laws to develop proposed legislation designed to hold banks and other third-party businesses accountable. Politically, few elected officials would object to combating human trafficking and legislation can easily be proposed at the state and federal levels. The financial costs of conducting trafficking would dramatically increase if traffickers were forced to seek alternatives to formal banks and invest in different properties rather than relying upon the hotel industry. Human trafficking is already immoral; however, making it unprofitable and increasing its risk is the key to ending the practice. While demand for trafficking will never entirely disappear, the profit margins of the crime can be substantially reduced as costs increase. Creating risk for secondary and tertiary actors, aside from the traffickers themselves, imposes more costs on traffickers as they will be forced to operate more aspects of the business directly. Holding third parties liable through civil cases and having such suits grounded in statute offer a viable path forward to creating these costs.

Dr. Ian Oxnevad, consultant, editor@acams.org

[1] Nate Gartrell, "Bay Area man made $21 million operating international sex trafficking websites that included child victims, feds say," *The Mercury News*, June 18, 2020, https://www.mercurynews.com/2020/06/18/bay-area-man-made-21-million-operating-international-sex-trafficking-websites-that-included-child-trafficking-victims-feds-say/ (accessed June 29, 2020).

[2] Ibid.

[3] "2019 Trafficking in Persons Report," *U.S. Department of State*, June 2019, https://www.state.gov/wp-content/uploads/2019/06/2019-Trafficking-in-Persons-Report.pdf (accessed June 29, 2020).

[4] "Anti-Terrorism Act (ATA)," *Osen LLC*, https://www.osenlaw.com/practice-areas/anti-terrorism-act-ata, (accessed July 6, 2020).

[5] Chiquita Case, *Osen LLC*, https://www.osenlaw.com/case/chiquita-case (accessed July 6, 2020).

[6] Ibid.

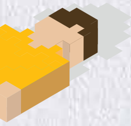
[7] Ibid.

[8] Corinne Ramey, "Lawsuits Accuse Big Hotel Chains of Allowing Sex Trafficking," *The Wall Street Journal*, March 4, 2020, https://www.wsj.com/articles/lawsuits-accuse-big-hotel-chains-of-allowing-sex-trafficking-11583317800, (accessed July 6, 2020).

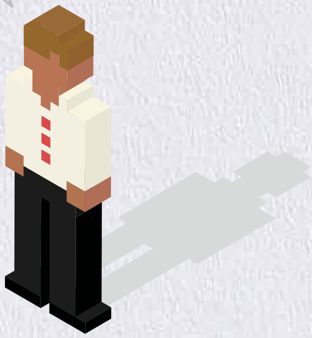
[9] "CS/CS/CS/HB 851 — Human Trafficking," *Florida Senate*, https://www.flsenate.gov/PublishedContent/Session/2019/BillSummary/Criminal_CJ0851cj_0851.pdf, accessed July 6, 2020.

FILTERING HIGH-RISK CUSTOMERS

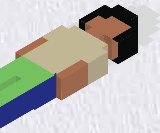
NO TECHNOLOGY REQUIRED



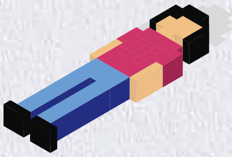
"The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of risk-based CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing."[1] In the U.S., financial institutions (FIs) are expected to maintain a customer due diligence (CDD) process that is risk-based and includes identifying and monitoring customers that present a higher risk for money laundering and other financial crimes. Though examination guidelines are explicit in what is expected, the details of what to cover in the monitoring and how to perform the monitoring are left to each FI to determine. Even for the most experienced Bank Secrecy Act (BSA) officer, ensuring their FI's Bank Secrecy Act/anti-money laundering (BSA/AML) program is sufficiently risk-based and that the enhanced due diligence (EDD) program is not excessively inclusive of low/moderate risk customers is not an easy task.



Identifying higher risk customers

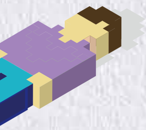


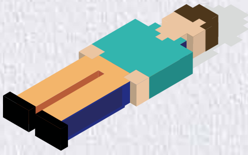
In short, a higher-risk customer is a customer who presents a higher risk for money laundering, terrorist financing or other financial crimes. This begs the question, higher than what? Higher than moderate or low-risk customers, but even this does not provide a complete answer. In actuality, a higher-risk customer exhibits a number of characteristics that have a high association with money laundering, terrorist financing or other financial crimes; these customers also exceed the FI's risk tolerance for the number of characteristics exhibited or the degree to which one or more characteristics is exhibited. A BSA officer using a single trait—such as a North American Industry Classification System (NAICS) code or a politically exposed person (PEP) status—to define their higher-risk customer base in the EDD program has likely not appropriately assessed the FI's high-risk customer risk.



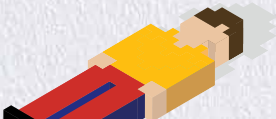
For example, a foreign national student from a designated higher-risk country receives monthly wire transfers from an apparent relative located in the high-risk country. This customer may be designated high risk for money laundering in a bank's anti-money laundering (AML) program solely because of the nexus to the higher-risk country. Now, consider a local dog groomer with no known ties to the higher-risk country that receives the same volume and dollar amount of monthly transfers from the higher-risk country. The dog groomer may also be designated high risk due to the nexus to the higher-risk country. Both customers are risk-rated "high" but do they both truly represent a higher risk of money laundering or other financial crimes to the FI? Absolutely not. To assess a customer's risk appropriately, an AML program must evaluate multiple characteristics of the customer holistically.

Defining risk characteristics





While almost all banking products can be used in the money laundering cycle, some products are more susceptible to money laundering. Historically, FIs use characteristics listed in the Federal Financial Institutions Examination Council (FFIEC) "Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual"[2] as a foundation for defining which characteristics are prevalent in money laundering.

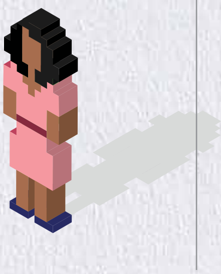


The manual lists over 30 risks associated with money laundering and terrorist financing[3] including products, services and customer types. The identified risks include such characteristics as non-U.S. residents and foreign individuals, lending activities, and trust and asset management services. Does this mean every non-U.S. resident is higher risk for money laundering? No. Is every lending or trust customer a higher risk for terrorist financing? Certainly not. Does a non-U.S. resident customer with a lending and trust relationship represent the highest risk of money laundering or terrorist financing? Not even close. So, how does a BSA officer holistically evaluate risk characteristics to identify customers presenting high risk to the institution appropriately?

The characteristics defined in the FFIEC manual are easily identifiable for FIs when onboarding customers and thus quantifiable for risk-scoring purposes. This point is critically important because the CDD Final Rule[4] requires covered FIs to include "risk-based procedures for conducting ongoing customer due diligence, to include understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile."[5] Often it is the information gathered at account opening, along with expected activity also collected at account opening, that defines the customer's perceived money laundering risk to the institution.

While a quantified risk profile calculation is not required nor implied by the regulation, many FIs use a risk score to identify its higher-risk customers. It is these higher-risk customers on which the FI will perform ongoing monitoring and conduct EDD.

EVEN GOOD CUSTOMERS PRESENT A CERTAIN LEVEL OF MONEY LAUNDERING RISK



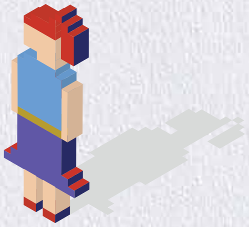
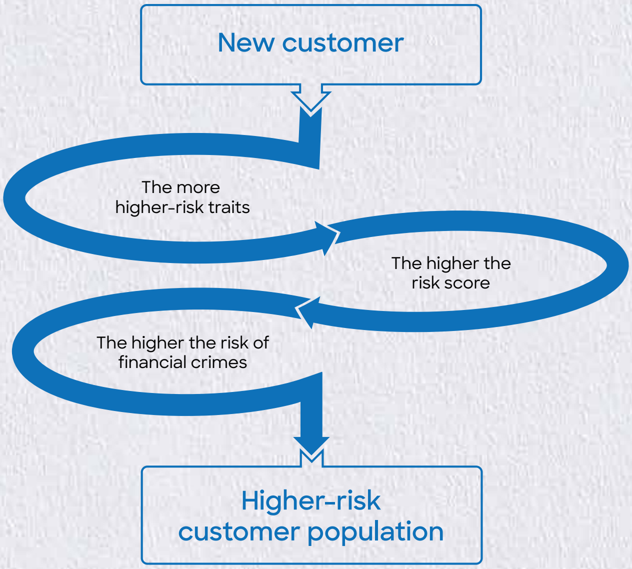


Figure 1:


New customer
The more higher-risk traits
The higher the risk score
The higher the risk of financial crimes
Higher-risk customer population

Risk mitigation

Figure 1 above is familiar and often accepted by auditors and examiners without question as presenting a risk-based approach to establishing customer money laundering risk. However, it is not the only way to identify customers as being higher risk for money laundering and is certainly not the most efficient for the institution as it will likely result in an excessive number of designated high-risk customers.

Consider merging the factors in Figure 2 (see page 38) with Figure 1 (using the risk characteristics outlined in the FFIEC manual) to define the potential money laundering risk of a customer further. To conduct a more accurate risk assessment, take the population of designated high-risk customers using the FFIEC risk characteristics and further stratify based on the institution's knowledge and experience with the customer. After all, if a book should not be judged solely by its cover, FIs should not judge a customer solely by their NAICS code, PEP status or nationality.

Known customers

Ask any customer-facing bank associate about a customer and chances are the response will be universal—"They're a good customer." But even good customers present a certain level of money laundering risk. The art of the AML profession is being able to determine which of those "good" customers present the highest level of risk to the institution accurately. It all starts with knowing your customer.

Know your customer (KYC) is generally comprised of three parts:

- Customer acceptance policy
- Customer identification processes
- Transaction monitoring (TM)

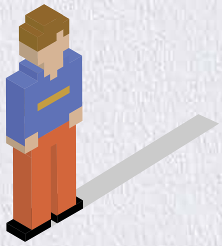
While customer acceptance and customer identification are critical factors in getting to know a customer, TM plays a large part in identifying higher-risk customers. Effective risk-based TM that results in a written comprehensive risk analysis of the alerted customer is an extremely effective risk mitigation tool. Therefore, an AML program should not only rely on its TM processes to identify potentially reportable activity but also to filter customers from its EDD pool of higher-risk customers effectively. A customer who has been reviewed by a BSA officer can be more appropriately risk-assessed than a customer who has solely been assessed at account opening based on the higher-risk traits outlined in the FFIEC manual.

A customer presenting the greatest risk of money laundering to the FI may be the customer who has never been on the bank's radar. A designated low-risk customer that has never been subject to a TM alert review or other review by the BSA team (e.g., onboarding review) may slip through many controls as a result of the lower-risk designation. Therefore, once the BSA team has come to know (through TM) a customer initially designated higher risk, the BSA officer might likewise consider re-evaluating the customer's high-risk designation.

Assuming an FI has a vigorous credit review program in compliance with the May 2020 "Interagency Guidance on Credit Risk Review Systems,"[6] certain loan customers carrying an initial high-risk designation may also be a candidate for a risk releveling.

TIP:

Put that 95% TM alert false positive rate to use in the high-risk customer identification process! Use alert reviews to filter customers presenting a lower risk than initially assigned

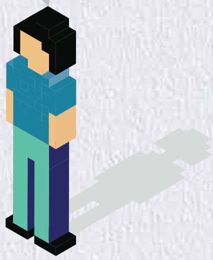


No money to launder

Accounts with minimal balances and minimal transactions are lower risk for money laundering. Remember, the primary purpose of money laundering is to disguise the proceeds of illegal funds into assets that look legitimate. When there are minimal funds involved and minimal opportunity to launder those funds, the risk of money laundering decreases. For accounts initially designated higher risk by an automated process due to the weight of nontransactional factors—like the customer being a non-U.S. resident or the customer belonging to a higher-risk NAICS code—the BSA officer should likely consider releveling the risk when transactional volume mitigates money laundering risk.

TIP:

Use loan reviews to filter customers presenting a lower risk than initially assigned.



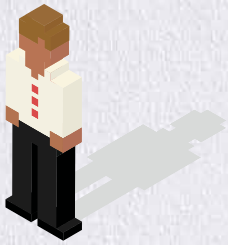
Self-regulatory organization oversight

A self-regulatory organization (SRO) is an entity that has the power to create and enforce industry regulations and standards. The SRO may outsource the oversight responsibility to other organizations. Examples of SROs in the U.S. are the Financial Industry Regulatory Authority (FINRA), the American Council of Life Insurers and the New York Stock Exchange.

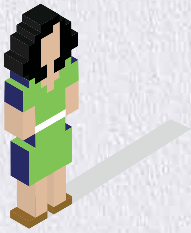
So, while a registered investment advisor or company may present a higher risk of money laundering—due to the large amount of funds available, the velocity of trades and the potential for Ponzi activity— the industry watchdog (FINRA or the Securities and Exchange Commission, a governmental regulator) is theoretically monitoring for illegal and unethical activity. For example, FINRA has "...the ability to audit dealers and associated firms and to ensure compliance with the standards currently in place. The goal is to promote ethical industry practices and improve transparency within the sector."[7]

TIP:

Stratify accounts of high-risk customers based on the number and dollar amount of transactions. Use standard deviation to filter accounts representing minimal risk of money laundering due to minimal usage. Then consider lowering the risk of the "outliers" on the low usage end.



TIP:
Consider using SRO oversight as a mitigation factor when assigning high-risk designations to certain NAICS codes. Obtain a copy of the most recent SRO exam report at onboarding and periodically afterwards.

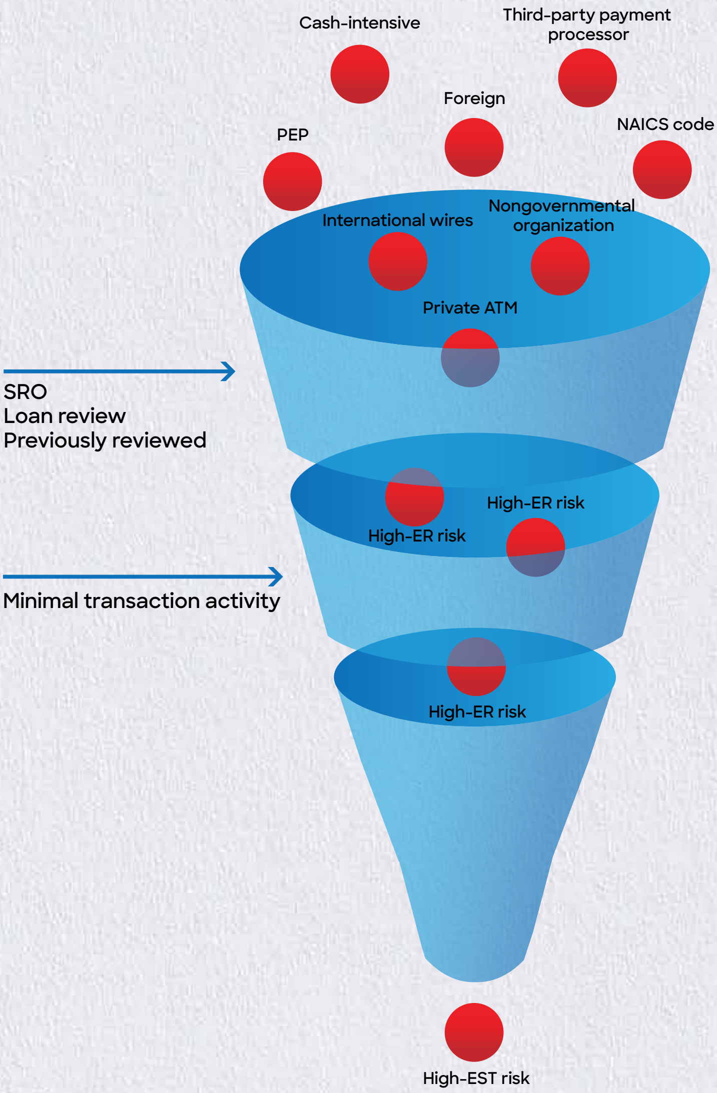


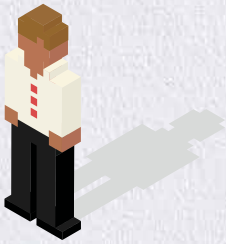
Likewise, while money services businesses (MSBs) are licensed by the Financial Crimes Enforcement Network (FinCEN),[8] FinCEN has delegated examining the AML programs of MSBs to the IRS.

The money laundering risk of a customer subject to SRO licensing and/or monitoring should logically be perceived as being mitigated by the SRO. Therefore, the risk to the FI of the customer should be less than that of a customer not subject to SRO oversight (e.g., businesses in industries with no guardrails). Or to flip this around, customers not subject to SRO oversight can be considered inherently higher risk for money laundering than those under an SRO.

Figure 2:

High-risk customer population





The importance of filtering high-risk customers

Filtering the higher-risk customer population down to those customers who truly represent high risks of money laundering or other financial crimes is important on many levels. The effect of filtering on risk management is threefold:

1. A more accurate reflection of the assessment of customer risk for the organization, which eliminates the artificially high rate resulting from including all customers in the designated characteristics
2. A lower false positive rate for high-risk customer designations, resulting in more meaningful EDD reviews
3. Efficiency gains freeing resources to expand the monitoring program

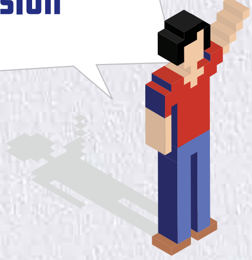
Implementing the filtering approach goes to the very heart of the "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing" from December 2018.[9] Specifically, regulators "… encourage banks to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their Bank Secrecy Act/anti-money laundering (BSA/AML) compliance obligations, in order to further strengthen the financial system against illicit financial activity."[10] The statement also underscores that banks will not be subject to supervisory action if the filtering program is implemented but ultimately unsuccessful. Finally, for community banks that may not have the resources to innovate on the technology side, this program enhancement requires little to no technology or IT support to implement.

Filtering the high-risk customer population provides clear evidence of a risk-based process in an AML program. Defining and documenting a method to remove the customers with mitigation factors from the high-risk customer list results is, in effect, risk-rating your high-risk list. The results from the filtering leave the riskiest of the high-risk customers ("high high") on which enhanced reviews should be targeted.

Finally, the April 2020 FFIEC Interagency Statement[11] announcing updates to the FFIEC manual is clear that, moving forward, examiners must focus on risk rather than technical precision. Examiners should take a risk-focused approach to reviewing an institution's BSA and AML programs.

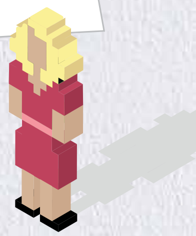
Amy Murphy, editor@acams.org

MOVING FORWARD, EXAMINERS MUST FOCUS ON RISK RATHER THAN TECHNICAL PRECISION



Takeaways

- Efficiency gains allow resources to be focused on truly higher-risk customers.
- Innovation can demonstrate the BSA officer's commitment to program improvements to examiners and the board.
- A risk-based process exhibits alignment with the BSA/AML program guidance.
- Appropriate assessment of risk may lead to better targeted examinations.



[1] "Customer Due Diligence – Overview," *Federal Financial Institutions Examination Council*, May 5, 2018, https://www.ffiec.gov/press/pdf/Customer%20Due%20Diligence%20-%20Overview%20and%20Exam%20Procedures-FINAL.pdf

[2] "BSA/AML Examination Manual," *FFIEC BSA/AML Examination Manual*, https://bsaaml.ffiec.gov/manual

[3] "Risks Associated with Money Laundering and Terrorist Financing," *FFIEC BSA/AML InfoBase*, https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/29

[4] "Customer Due Diligence Requirements for Financial Institutions," *Federal Register*, May 11, 2016, https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf

[5] Ibid.

[6] "Credit Risk: Interagency Guidance on Credit Risk Review Systems," *Office of the Comptroller of the Currency*, May 8, 2020, https://occ.gov/news-issuances/bulletins/2020/bulletin-2020-50.html

[7] Adam Hayes, "Self-Regulatory Organization—SRO Definition," *Investopedia*, https://www.investopedia.com/terms/s/sro.asp

[8] "MSB Registrant Search," *Financial Crimes Enforcement Network*, https://www.fincen.gov/msb-state-selector

[9] "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," *Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency*, December 3, 2018, https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20(Final%2011-30-18)_508.pdf

[10] Ibid.

[11] "April 2020 Updates to the Bank Secrecy Act/Anti-Money Laundering Examination Manual," *Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee*, April 15, 2020, https://www.ffiec.gov/press/PDF/Interagency%20Statement.pdf

50 YEARS OF BSA:

FROM DORMANCY TO ZEAL

Author's note: This is the first in a series of articles covering the comprehensive history of the Bank Secrecy Act (BSA). Read the rest on ACAMSToday.org.

In terms of historical events, many things happened in 1970. The U.S. military invaded Cambodia; Americans watched in horror as the Apollo 13 mission was aborted, but the crew returned safely to Earth; members of the Ohio National Guard fired into the crowd of Kent State University demonstrators; and the Vietnam War protests reached a fever pitch. On the pop culture side, music fans received troubling news from Paul McCartney that The Beatles had disbanded.

Also in 1970—and by no means newsworthy compared to other transpiring events—the U.S. Congress enacted the Currency and Foreign Transaction Reporting Act, commonly referred to as the Bank Secrecy Act (BSA). Few laws can lay claim to engendering such paradigm shifts in the financial services industry and profoundly influencing the way law enforcement combats criminal activity. With a regulatory framework now mirrored by other nations, today the BSA stands as a much relied upon sentry in protecting the nation's financial highways from rogue actors, organized crime and terrorist financing.

However, the BSA did not begin with such ambition. The tale of the BSA in the early years can best be described as a game of cat and mouse.

Advantage, mouse

Since the takedown of Al Capone, the U.S. federal government found that using income tax laws often proved to be the only effective way well-insulated crime bosses, who used their minions to carry out their felonious acts, could be brought to justice.

As Treasury agents got better at following the money, organized criminals got better at hiding the money. Buoyed by cunning attorneys and accountants, criminal organizations eventually evolved their money laundering into seasoned best practices. This included depositing copious amounts of currency in nominee bank accounts then transferring funds to shell entities. It also included using couriers to transport suitcases of currency offshore to countries that prided themselves on absolute banking secrecy.

By the late 1960s, criminal groups began to flourish as they availed themselves of income streams from the burgeoning narcotics and marijuana trade. In 1968, a group of law enforcement officials led by U.S. Attorney Robert Morgenthau of the Southern District of New York pleaded with the Senate Committee on Banking for help "in tracking transactions that were facilitating organized crime, drug operations and tax evasion."[1]

50

Advantage, cat

The enactment of the BSA in 1970 followed extensive hearings concerning the lack of records for foreign and domestic customers thought to be engaged in illegal activities. But it was not only the concerns of law enforcement that led to its passage. By 1970, the U.S. had entered a recession and the government faced mounting debt associated with the Vietnam War. Congress also had a keen interest in using the BSA to reduce deficit spending by reigning in tax evasion.

The purpose of the BSA was to hand regulators and law enforcement a tool to obtain financial information having "a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[2]

The BSA required banks to file reports for currency transactions over $10,000 to the Treasury. To assist law enforcement with identifying those depositing funds of suspicious origins, the new law included a record-keeping mandate to maintain records of their customers' identity and microfilm certain transactional documents and records. To address the money mules shuffling funds overseas, the BSA required reports for transporting currency exceeding $5,000 into or out of the country. And to identify those utilizing secret offshore accounts, the law required individuals to report ownership interest in foreign bank accounts on a tax return form.

Banks' vocal opposition

The passage of the BSA drew fierce opposition from the banking community, leading to a lengthy legal battle that culminated in a Supreme Court showdown in 1974. The high court held that Congress properly exercised their power "to deal with the problem of crime in interstate and foreign commerce."[3] Furthermore, the court held that, "the regulations for the reporting by financial institutions of domestic financial transactions are reasonable, and abridge no Fourth Amendment rights of such institutions, which are themselves parties to the transactions involved." As it relates to banking patrons, the high court concluded, "a depositor plaintiff incriminated by evidence produced by a third party sustains no violation of his own Fifth Amendment rights."[4]

When the Supreme Court finally upheld the BSA, it seemed that the cat had finally gained the upper hand. However, the cat was highly dependent on banks to set the mousetraps and banks were rather uncomfortable being rodent detectors. Banks now had to inquire with their depositors about their identity and the nature of their currency transactions.

A tradition of banking

In 1975, only a paltry 3,418 currency transaction reports (CTRs) were filed. Banks spent little effort in deploying policies and procedures to ensure they identified and reported currency transactions. Responsibility for filing the form often fell to the line teller, with no supervisor review. Bank employees, for the most part, received inadequate training, and senior banking officials did not stress to their organizations the importance of the BSA in catching the criminals.

The BSA cut against the grain of centuries-old banking tradition—keeping customers' financial matters private. This pillar of banking etiquette conditioned banks not to make too much of a fuss about compliance. Bank officials were particularly sensitive to how customers and shareholders would perceive the new mandate.

However, not all those that deal in large quantities of currency are up to funny business. To reduce the number of CTRs, the BSA allowed banks to exempt certain customers from CTRs if, in their judgment, the currency was commensurate with the nature of their business. However, the original law afforded considerable latitude to banks in making this determination, which became a convenient excuse to avoid reporting on currency. And some of those exempted from CTRs were members of criminal enterprises.

Examining the mousetraps

The cat also relied on bank examiners to validate that the banks were properly calibrating the mousetraps. But the examiners, for the most part, did not even inspect the mousetraps.

The Office of the Comptroller of the Currency (OCC) had been delegated the authority to examine banks for BSA compliance. As Congress later confirmed, OCC bank examiners were not properly trained on the BSA, and in some instances, examiners were not aware of the BSA's requirements. The OCC audit procedures did not root out material violations of the law.

THE PASSAGE OF THE BSA DREW FIERCE OPPOSITION FROM THE BANKING COMMUNITY

Tradition also did not serve the OCC. Understandably, government bank examiners felt their purpose in life had always been to ensure an FI's soundness. Redirecting examiners' time to validating BSA adherence did not fall within their perceived priorities. The BSA became just another box on a long list of "check the box" audit procedures.

In this spirit of laissez-faire compliance, diligence to the BSA never gained a foothold in the 1970s, but noncompliance did catch the attention of the IRS Criminal Investigation (IRS-CI).

In 1977, two former Chemical Bank officials pleaded guilty to income tax charges stemming from cash-changing operations for narcotics dealers at two of the bank's branches in the Bronx. Both admitted they exchanged large denomination bills with smaller denominations, making it easier for the narcotics dealer to send the money out of the country for deposit in the Caribbean. Soon after, Chemical Bank was indicted on failure to report more than 500 cash transactions that amounted to $8.5 million.

IRS-CI began to pursue other banks that committed felonious violations of the BSA, but the penalties brought upon those financial institutions (FIs) amounted to a slap on the wrist compared to today's consequences.

Congress takes notice

The bank examiners' casual approach to dealing with the BSA eventually caught the eye of Congress. During hearings before the Senate Banking Committee in 1980, the enforcement efforts of the oversight agencies were described as "dismal" and "lackadaisical." This description would comport with a U.S. Government Accountability Office report that found "the compliance monitoring of the bank regulatory agencies was inadequate, cursory or nonexistent."[5]

In response to fractured compliance efforts noted by Congress, the Treasury updated BSA regulations to tighten up requirements on the rules on exempting customers. The only exemptions allowed were retail establishments expected to have substantial cash transactions as a normal course of business. Banks also had to document the exemption and provide a list of such exemptions to the Treasury upon demand.

In 1981, the Treasury also provided bank supervisory agencies with more robust procedures to inspect the BSA mousetrap. The Treasury believed that "if a bank examiner follows the entire set of procedures, there is a high probability that any major incident of noncompliance at a financial institution will be detected."[6] But adoption of the revised examination procedures progressed slowly.

Operation Greenback

By 1980, America saw the rise of even bigger criminal enterprises ruled by ruthless international kingpins like Carlos Escobar, whose henchmen caused the murder rates in Miami to skyrocket. Escobar found a very friendly FI, Bank of Credit and Commerce International (BCCI), that was more than willing to help the drug overlord *Forbes* labeled one of the richest men in the world.

The Treasury made the eye-popping discovery of a surplus of $6 billion floating around in Florida banks. According to Miami IRS Special Agent Michael McDonald, "The money was coming in down here in suitcases and duffel bags to pay for the cocaine."[7] Recounting the situation, McDonald said, "It wasn't until the drug war hit South Florida that we looked at the Bank Secrecy Act, as we called it, and the tracing of currency to look at these reports. That's when we realized banks aren't filing them – not just in Miami but all over."[8] By 1979, the total number of CTRs filed by banks amounted to a minuscule 121,000.

Along with his U.S. Customs counterparts, McDonald helped form the first money laundering task force in South Florida known as Operation Greenback. Greenback targeted attorneys, accountants, money brokers, money couriers and bankers. It documented $2.6 billion in laundered currency through 16 narcotics organizations and netted 164 arrests, 211 indictments and 63 convictions. The *crème de la crème* was the takedown of BCCI, which *Time* called, "The Dirtiest Bank of All."

BY 1979, THE TOTAL NUMBER OF CTRS FILED BY BANKS AMOUNTED TO A MINUSCULE 121,000

A consummate collaborator, McDonald shared his best practices with other agents throughout the country. Richard Speier—newly minted Los Angeles (LA) IRS group supervisor—recalled being so inspired by McDonald, he turned his entire group into a pure Title 31 financial investigation task force. Speier's agents followed the influx of Columbian drug money into LA banks by smurfs, which was then converted into cashier's checks and wire transfers all destined to Miami. It was like walking into an orchard with well-ripened, low-hanging fruit; the stats his group generated greatly pleased his boss. According to Speier, "We got our leads exclusively from bank operations officers and bank security departments."[9] However, Speier ran into roadblocks when bank legal counsel occasionally jumped into the fray to protest the voluntary disclosures of customer information.

Miami and LA were not the only regions where banks resisted making BSA filings. One glaring example was the First National Bank of Boston (FNBOB), which audaciously failed to report $1.2 billion in currency transactions, much of which was $20 bills stuffed in bags emanating from Swiss banks. The bank also graciously granted exemptions on businesses associated with a notorious crime family.

THE COMMISSION EXPRESSED A CONCERN THAT THE BSA DID LITTLE TO DISSUADE BANK REPRESENTATIVES FROM WILLFULLY PROVIDING MONEY LAUNDERING SERVICES TO BAD ACTORS

The early 1980s marked a rapid increase in the number of FIs under criminal investigation for violations of the BSA. Though the cases got media attention, the penalties dished out for BSA violations were apparently not onerous enough to illicit corrective behavior. IRS-CI continued to identify banks with big problems and complicit employees.

1984: Making the cash connection

The work of McDonald's Greenback certainly grabbed the attention of officials in higher places. In October 1984, President Ronald Reagan's Commission on Organized Crime issued a bold report on the state of criminality in the U.S. titled, "The Cash Connection: Organized Crime, Financial Institutions and Money Laundering."

The report acknowledged that the BSA had been a "potent weapon against money laundering activities," so the commission concluded that there are aspects of the law that have encumbered the BSA's effectiveness. As the report reads, "willful violations of the Act are not stringent enough to accomplish their intended purpose, and the felony provisions of the Act can be applied only in extremely limited situations."[10]

The commission expressed a concern that the BSA did little to dissuade bank representatives from willfully providing money laundering services to bad actors. As the report stated,

> "Even though money launderers have corrupted, or attempted to corrupt, officials and employees of numerous financial institutions in conducting their money laundering activities, the Bank Secrecy Act provides neither civil nor criminal penalties for such conduct, and the penalties under the existing Federal criminal statute for bribery of bank officials are far too lenient."[11]

A trip to the woodshed

Since early 1984, a Senate banking subcommittee had been holding hearings on offshore banking and money laundering. Not surprisingly, the plea of the FNBOB got their attention. Stewing with disappointment, the committee not only called the president of FNBOB to testify but also the head of the OCC for failing to detect odious behavior.

In his subcommittee opening remarks, Congressman Fernand St. Germain said, "Fourteen years ago, the Committee on Banking attempted to draft the banking industry and its Federal regulators for a war on organized crime, drug traffickers, tax evaders, and an assortment of white collar frauds. It is obvious that some have managed to dodge that draft." St. German added, "If the Bank of Boston case is indicative of a cross section of compliance and enforcement, then we are seeing an industry and a regulatory structure render a major law enforcement tool a virtual nullity."[12]

Redirecting his shellacking to bank examiners, St. Germain said, "The Office of the Comptroller of the Currency sent its examination force into the Bank of Boston every year. It never found a problem with the compliance with the Bank Secrecy Act, not a thing, all the while the unreported transactions and the outlandish list of exemptions were piling up."[13]

On the governmental side, St. Germain's disappointment was not limited to the OCC. He also pointed out, "the Federal Reserve also has failed to cover itself with glory in these episodes."[14]

A mea culpa

The chairman of FNOB, William L. Brown, told the subcommittee, "The events of the past several weeks have taught us a painful lesson; they have taught us that we must redouble our efforts to ensure that all our employees and officers, at every level, abide by both the letter and spirit of the law." Brown further stated, "We must also recognize that financial institutions have a moral and ethical obligation to assume a greater degree of responsibility for identifying possible illegal activity."

The wind of media attention filled the sails of subcommittee members as they took banks to task. As one committee member said, "barely a day passes that a leading newspaper or magazine does not have some article bringing out new charges, new allegations." For the first of the hearings, *The Wall Street Journal*

published an article entitled, “How the Mob Is Using Financial Institutions To Disguise its Gains.” The subtitle to the article read, “Banks Eager for the Business; Aren’t Suspicious Enough Up Front.”[15]

The mousetraps to end all mousetraps

The findings from Operation Greenback and “The Cash Connection” report, and the subcommittee hearings on the FNBOB created powerful momentum for new legislation. In 1986, First Lady Nancy Reagan and President Reagan appeared in a nationally televised event to kick off the first lady’s “Just Say No” to drugs campaign. That same year, President Reagan sent a resounding messaging of “Just Say No” to money laundering by signing into law the Money Laundering Control Act (MLCA) of 1986.

The MLCA made the act of money laundering a federal crime with significant prison time. It also prohibited structuring transactions from evading CTR filings. Anyone facilitating this money laundering, including bank employees, would suffer the same fate with a conspiracy charge. MLCA directed banks to establish and maintain procedures for complying with the reporting and record-keeping requirements of the BSA.

The MLCA brought vibrancy to BSA compliance efforts by imposing significantly more consequences on those within an FI for turning a blind eye to BSA.

In less than a decade, BSA compliance efforts went from dormancy to zeal.

Final thoughts—Part 1

In 1986, the theme song to the hit TV series “Miami Vice” was so popular, it garnered two Grammy Awards and was voted the No. 1 theme song of all time by *TV Guide* readers. As one of the most watched programs during the 1980s, “Miami Vice” put the sensationalism of the drug wars in America’s face each week. The violence and financial audacity of drug kingpins portrayed in the show, according to law enforcement, mostly tracked with reality.

As a newly created law, MLCA entered the world at a time when the public, Hollywood and elected officials were all in on the war on drugs. Significant enforcement resources were thrust into the enforcement of the MLCA and criminal violations of the BSA.

But the smarter criminals learned to adapt to their new environment. There were still ample opportunities to launder with nontraditional FIs to expend their felonious financial highways. These establishments rarely, if ever, got their mousetraps inspected by government examiners.

And so, the cat and mouse game continued.

Paul Camacho, CAMS, retired special agent in charge, IRS Criminal Investigation; member of the board of directors, The Mob Museum

[1] *Subcommittee on Financial Institutions Supervision, Regulation, and Insurance*, April 3, 1985.

[2] “31 U.S. Code § 5311.Declaration of purpose,” *Legal Information Institute*, https://www.law.cornell.edu/uscode/text/31/5311#:~:text=It%20is%20the%20purpose%20of,including%20analysis%2C%20to%20protect%20against

[3] California Bankers Assn. v. Shultz, 416 U.S. 21 (1974).

[4] Ibid.

[5] U.S. Senate hearings, *Permanent Subcommittee on Investigations of the Committee on Governmental Affairs*, March 12, 1985.

[6] Ibid.

[7] Howard Cohen, “Mike McDonald, an IRS agent who busted Cocaine Cowboys, dies at 68,” *Miami Herald*, October 25, 2016, https://www.miamiherald.com/news/local/obituaries/article110462902.html

[8] Ibid.

[9] Interview with Rick Speier, July 6, 2020.

[10] Ibid.

[11] Ibid.

[12] U.S. Senate hearings, *Permanent Subcommittee on Investigations of the Committee on Governmental Affairs*, April 3-4, 1985.

[13] Ibid.

[14] Ibid.

[15] Ibid.

Render unto OFAC

CAATSA limits the president's ability to relax sanctions that are already in place

When the U.S. Congress enacts sanctions by passing legislation, it is often unwelcome by the executive branch. Such legislation can restrict the flexibility and autonomy of the executive branch in responding to changed diplomatic circumstances when trying to advance U.S. foreign policy goals. That was certainly the case during the Obama administration, whose ability to relax sanctions imposed on Cuba was limited by previously enacted congressional acts. Similarly, Title II of the Countering America's Adversaries Through Sanctions Act (CAATSA)—which imposes new sanctions on parties associated with the Russian Federation—appears specifically designed with President Donald Trump in mind. In addition, CAATSA limits the president's ability to relax sanctions that are already in place, which seems to have been an attempt by Congress to restrain the president's apparent reticence toward being assertive with Russia, as evidenced by his unwillingness to confront President Vladimir Putin about Russia's interference in the 2016 presidential election.

Therefore, it is interesting to analyze such laws through the lens of congressional intent and then predict how the powers given to the administration will likely be utilized because of, or despite, the letter of the law. A prime example of this is the Caesar Syria Civilian Protection Act (Caesar Act), which was passed as part of the National Defense Authorization Act for Fiscal Year 2020 (NDAA).

What is in the law?

The Caesar Act contains both punitive measures and measures intended to assist Syria's civilian population. The punitive measures are twofold. First, the U.S. secretary of the treasury was directed to determine within 180 days whether or not the Central Bank of Syria (Central Bank) should be designated a financial institution (FI) of primary money laundering concern (PMLC). If he makes that determination, he is required to impose sanctions as described in Section 311 of the USA PATRIOT Act.

Secondly, sanctions can be imposed on foreign persons if they:

- Provide support (financial, material or technological) or have a significant transaction with the Syrian government (including senior officials of that government); parties who are involved in military capacities within Syria for the Syrian government, Russia or Iran; or parties sanctioned under the U.S.' Syria or Syria-related sanctions
- Sell or provide goods or services that enable the Syrian government to maintain or expand their domestic petroleum and natural gas production
- Sell or provide aircraft or aircraft parts, or provide goods or services for operating aircraft, for military use within Syria for the Syrian government to anyone operating in areas controlled by the government or with other forces allied with it
- Provide construction or engineering services to the Syrian government

The act also includes a "Sense of Congress" section that suggests that the president should include loans, credits or export credits when defining what constitutes "financial support."

The sanctions that are to be imposed include asset freezes, a ban from admission into the U.S., denial of new visas and revocation of existing ones.

The act also makes comparatively minor amendments to the Syria Human Rights Accountability Act of 2012. Most notably, the amendments add a list of specific Syrian government roles for the president to consider for inclusion in the list of persons that the law requires be submitted to Congress.

Why was it passed?

The "Caesar" in the legislation's title refers to the code name of a military defector who smuggled a trove of thousands of photographs that documented extensive human rights abuses (including torture and starvation) and deaths of persons detained by the Assad regime from March 2011 to August 2013. It was originally filed in the House of Representatives in July 2016 by Rep. Eliot Engel (D-NY) after Caesar testified and shared some of the photographic evidence before Congress in 2014. However, various versions of the bill repeatedly failed to pass Congress for a variety of reasons, including objections to other unrelated provisions in larger legislative packages in which it was included, and a lone senator's objection to unanimous consent for the bill based on his desire to proceed with diplomatic measures rather than mandating coercive ones.

The version that ultimately passed was introduced on January 3, 2019, coincidentally close on the heels of President Trump's December 2018 announcement of a withdrawal of U.S. combat troops from Syria. That decision by the president played a part in Senate Majority Leader Mitch McConnell expressed opinion to throw his support behind the bill.[1] Due largely to efforts by Senator McConnell's office, the Caesar Act became a part of the NDAA for 2020, a "must-pass" bill that eventually passed and was signed into law on December 20, 2019. So, while the original impetus for the bill's passage was the outrage over the human rights abuses of the Syrian regime, ultimately it was Congress' perceived need for greater influence in Syria, a country in which the U.S. had ceded the battle on the ground to nations not aligned with U.S. foreign policy interests, that enabled it to finally become law.

The prospect of sanctions imposed on third parties is intended to have a chilling effect on Syria's current partners, both politically and economically

How could it be used (and how will it)?

The Caesar Act aims to pressure the Assad regime in a diverse set of ways. First, the law directs the secretary of the treasury to consider the imposition of Special Measures under Section 311 of the USA PATRIOT Act on the Central Bank. Special Measure 5, the most severe, would prohibit all U.S.-organized banks and U.S. branches of foreign banks from offering correspondent services to the Central Bank. As a practical matter, it would also deny the Central Bank dollar-denominated accounts at other banks as well. Such a move by the Treasury would force the Central Bank to use less desirable currencies for any international trade transactions. The Central Bank is already sanctioned by the United Kingdom, European Union, Switzerland and Canada, which would force any financial services needs mostly to financial firms in the Middle East, Asia and Oceania. Therefore, with the possible exception of Chinese currency, financing Syrian trade flows would incur additional foreign exchange costs. This is due to the need to use currencies that are comparatively more volatile, or less easily convertible, than the U.S. dollar, which makes them more expensive to use (since potential foreign exchange losses due to volatility are factored into the exchange rates).

In addition, the prospect of sanctions imposed on third parties is intended to have a chilling effect on Syria's current partners, both politically and economically. According to the Observatory of Economic Complexity,[2] in 2018, Syria imported $6.21 billion in goods, with almost 60% of this roughly

evenly split between China, Turkey and the United Arab Emirates (UAE). Of the remainder, other countries in the Middle East comprised approximately 9%, and its close ally Russia contributed 3.67%. The latest figures for imported services from 2010 showed that the vast majority of Syria's $3.53 billion of imported services were for transportation ($1.59 billion), personal travel ($1.51 billion) and insurance services ($121 million).

Therefore, it is not unreasonable to assume that the Caesar Act is intended to give pause to existing major trade partners that could easily leverage existing economic ties to aid the Assad regime. However, each of the largest trade partners presents cause for concern. These countries were still exporting goods to Syria as late as 2018, despite the country's long-running civil war and the atrocities documented by Caesar years earlier.

Turkey has been used as a transit country for foreign terrorist fighters, and its purchase of Russian S-400 missiles makes it subject to sanctions under Section 231 of CAATSA. Similarly, companies in the UAE have been involved—as documented in multiple Office of Foreign Assets Control (OFAC) enforcement actions—in facilitating trade with Iran. Lastly, China has a long-standing record of being willing to allow its companies to continue to trade with North Korea. In addition, while not part of any original justification behind the composition of the law, the Caesar Act should also make China think twice about expanding its influence in Syria under its Belt and Road Initiative, as that would likely involve prohibited construction and engineering services. Given that the U.S. government has not been shy in imposing sanctions on individuals and entities on all three countries (although the Syria-related sanctions imposed on Turkish officials were not in place for very long), the Caesar Act is likely to make firms from these countries think twice before expanding their commercial ties. Even given countervailing geopolitical concerns (e.g., U.S. Air Force bases in Turkey) that may make OFAC think twice before making designations, the economic impact of designation by OFAC (and the knock-on avoidance of sanctioned parties by firms in mortal fear of being designated themselves) will undoubtedly be a factor to consider for firms that are contemplating Syrian business ties proscribed by the Caesar Act.

It is likely that the Caesar Act will be followed to the letter but not the spirit of the law

However, it is unclear whether the Caesar Act explicitly targeting assistance to the Iranian and Russian governments' military involvement within Syria will inhibit those nations (or firms that already trade with them) in any way. Given the extent of current Iranian sanctions and the fact that secondary sanctions are attached to parties designated by OFAC (including Iran's defense department, and the Islamic Revolutionary Guard Corps, or IRGC), it is unlikely that any firms currently conducting business with the Iranian government would cease doing so due solely because of the passage of this measure. Similarly, given the lack of a response to both India's and Turkey's purchase of S-400 missiles from the Russian firm Almaz-Antey (which appears on a Department of State list issued under Section 231 of CAATSA that bars third-party business with such firms, under penalty of menu-based sanctions) and the willingness of OFAC to give extended reprieves from sanctions to firms owned by Oleg Deripaska (a sanctioned Russian oligarch), any firms willing to aid Russian military forces in Syria will probably not be deterred by the Caesar Act. Similarly, given the transfer of the Venezuelan book of business from units of Rosneft to Russian state-owned companies has, to date, elicited no regulatory response from OFAC, the threat of sanctions is unlikely to stop Russian firms from aiding the Assad regime in cementing its grip on power.

Given this, what will likely occur as a result of the passage of the Caesar Act? The first glimpses of actions taken under this authority are quite limited but are not heartening. The June 17 OFAC designations were largely made under the authority of executive order 13894, which targets human rights abuses and officials of the Turkish government, rather than the Caesar Act. Of the handful of entities sanctioned with the SYRIA-CAESAR sanctions program tag, all were Syrian firms involved in real estate activities, with one also being involved in building construction. The three individuals sanctioned under the Caesar Act sanctions on that date were all Syrian nationals, although two of them had connections to Canada. While consistent with the letter of the law, designation of domestic Syrian parties is clearly at odds with congressional intent, as seen in the targeting of "foreign" parties (as opposed to "Syrian") for sanctions designations in the legislation.

In addition, as of July 6, the determination of whether or not the Central Bank is an FI of PMLC appears not to have been made, despite the 180-day deadline mandated by the law having passed over two weeks earlier. This lack of definitive action may be a deliberate ploy to thwart the will of Congress. By not making the mandated determination, the Trump administration can avoid congressional wrath (by not designating the Central Bank as an FI of PMLC), while also not forcing Russia to prop up Syria financially or to increase its military presence in the vacuum created by the Syrian government's decreased ability to finance its military operations due to the loss of correspondent services.

With a bang or a whimper?

The history of legislative sanctions laws is mixed. The ones that have more successfully tied the hands of the executive branch are those that include the imposition of trade bans, such as laws enacted that restricted trade with Cuba and Myanmar. On the other hand, the sections of Title II of CAATSA that dictate the imposition of sanctions on classes of parties have been shown to be relatively toothless three years after their passage since the legislation says the president shall impose sanctions without specifying a time frame for that action. The purchase of Russian S-400 missiles by Turkey without regulatory consequence, despite the clear language of Section 231 of the CAATSA statute is a notable example of this. In a similar fashion, a list of Russian oligarchs was apparently created from a list in a mainstream business publication, technically fulfilling the regulatory requirement under CAATSA to produce such a list, without following the spirit of the requirement (which would have necessitated an independent, rigorous research effort).

It is likely that the Caesar Act will be followed to the letter but not the spirit of the law as demonstrated by the designations made on June 17. Such divergences between congressional intent and executive branch action represents the defiance of the requirements imposed by a co-equal branch of government. Whether legislation imposing economic sanctions other than trade restrictions can be made impervious to presidential desires to ignore or subvert congressional intent is a question that will need to wait for a future bill landing on the White House's Resolute Desk; the Caesar Act does not meet that bar.

Eric A. Sohn, CAMS, CGSS, global market strategist and product director, Dow Jones Risk & Compliance, New York, NY, USA, eric.sohn@dowjones.com

[1] Mitch McConnell, "Mitch McConnell: Withdrawing from Syria is a grave mistake," *The Washington Post*, October 18, 2019, https://www.washingtonpost.com/opinions/mitch-mcconnell-withdrawing-from-syria-is-a-grave-mistake/2019/10/18/c0a811a8-f1cd-11e9-89eb-ec56cd414732_story.html

[2] *The Observatory of Economic Complexity*, https://oec.world

CRIMINAL PLOY OR JACKPOT JOY?

As there is a paucity of empirical data on money laundering and terrorist financing in the United Kingdom's (U.K.) online gaming sector, the evidence of actual criminal use in this industry remains sparse. The following Metropolitan Police Service (MPS) analysis seeks to address this issue by comprehensively evaluating 157 suspicious activity reports (SARs) provided by the online gaming sector. The analysis will assess how susceptible the online gaming sector is to money laundering by examining the following questions:

- What prompts the U.K. online gaming sector to disclose a SAR to the UK Financial Intelligence Unit (UKFIU)?
- Do operators know enough about their customers to allow intervention at an early stage to prevent money laundering or problem gambling?
- Is there evidence of criminals exploiting online gambling operators' anti-money laundering (AML) deficiencies?
- Does the analysis suggest the main money laundering risk is criminal lifestyle spending?
- Does lifestyle/problem gambling draw these people into criminality?
- Is the ease of gambling online leading to more female participants being reported?
- Are customers using stolen cards to gamble?
- Are Defense Against Money Laundering (DAML) SARs effective in disrupting money laundering and do they provide substantial value to law enforcement agencies (LEAs)?

The overall purpose of this MPS analysis is to develop a better understanding of the threat posed by money laundering and its predicate offenses to the online gaming sector. This analysis will also provide constructive feedback thereby enabling reporters to refine their systems, raise their level of reporting and produce better quality SARs.

The analysis

Gambling is a legitimate popular leisure activity in Britain. According to the Gambling Commission, Britain has the largest regulated

online gambling market in the world that generates 4.7 billion pounds ($6.1 billion) of gross gambling yield (GGY) per annum.[1]

Online gambling has grown significantly and, before COVID-19, the Gambling Commission estimated it was likely to increase from 34% to 50% of the total British market by GGY within the next few years.

Whilst recognizing that not all gambling operators are subject to money laundering regulations—which currently only apply to remote and nonremote casinos—all gambling operators that offer services in Britain must be licensed by the Gambling Commission, including operators based overseas that offer services to consumers in Britain.

Anti-money laundering and counter-terrorist financing (AML/CTF) compliance is a condition of the operating licenses issued by the Gambling Commission. Further, under the Gambling Act 2005, it is mandatory for gambling operators to comply with the licensing objectives to keep crime and its proceeds out of gambling. Finally, the Proceeds of Crime Act 2002 (POCA) places an obligation on all gambling operators to submit a SAR where operators know, are suspicious of, or have reasonable grounds for knowing or suspecting that a person is engaged in money laundering.

The SARs regime is the process by which the private sector discloses their suspicions of money laundering and terrorist financing to LEAs. In doing so, the regulated sector complies with their mandatory reporting obligations under POCA and the Terrorism Act 2000, and the information contained within the SARs provides opportunities for LEAs to intervene, disrupt and prosecute criminality.

It is important to recognize that SARs simply reflect a reporter's suspicions and that standards differ across institutions and sectors, so there is a lack of clarity as to what a financial practitioner would consider suspicious. Therefore, filing a SAR does not mean that money laundering activity has actually taken place.

According to the U.K.'s first and second national risk assessments of money laundering and terrorist financing, the gambling sector was overall less attractive to criminals than other sectors and less likely to be used for laundering a significant volume of criminal funds. The reports concluded that the overall money laundering and terrorist financing risks in the gambling sector are low. These reports also suggest that a significant proportion of the money laundering that occurs within the industry is by criminals who spend their proceeds of crime for leisure rather than for "washing" funds.

Due to the continued lack of evidence, the sector continues to be assessed as low risk for money laundering. Therefore, this SARs analysis seeks to confirm whether these assertions are correct or may require further validation.

Key findings following analysis of the 157 SARs submitted by the online gaming sector

- 2% of SARs concerned customers producing fraudulent documentation
- 6% of the reported individuals were disclosed due to inquiries by LEAs
- 6% of SARs concerned suspected mule accounts
- 8% of SARs involved funds placed with stolen bank cards
- 16% of the SAR subjects reported had committed a crime to fund their gambling addiction
- 20% of the SAR subjects reported were women
- 20% of the SAR subjects were reported for failing to engage in source of funds/source of wealth process[2]
- 27% of SARs were DAML SARs
- 52% of SAR subjects reported had been subject to previous SARs
- 53% of SAR subjects reported had no occupation shown
- 56% of SAR subjects reported had been previously arrested

Analysis of SARs submitted by the online gaming sector

This analysis focused on 157 SARs provided by 26 gaming operators between January 1, 2019, and July 14, 2019. The SARs identified 158 individuals that are residents throughout the U.K. with the largest groups located in London (29), Yorkshire (14), Kent (11), Lancashire (eight) and Essex (seven). Dates of birth ranged from 1949 to 2000 (with those born in 2000 all being women). The majority of SAR subjects (63) were born in the 1980s, the most popular year being 1989. Occupations provided included manager (10), company director (nine), unemployed (six), nurses/caregivers and gym workers (five).

Eight individuals did not list their address and 84 individuals did not list their occupation. This missing data is

THE REPORTS CONCLUDED THAT THE OVERALL MONEY LAUNDERING AND TERRORIST FINANCING RISKS IN THE GAMBLING SECTOR ARE LOW significant as it diminishes an operators' ability to conduct affordability assessments, identify problem gambling and consider changed financial circumstances.

Seventy-seven of these individuals were the subject of just one SAR. Eighty-one individuals were subject to a further 370 SARs collectively, and one individual had previous convictions for money laundering and had been reported 19 times. Information provided supported money laundering activity as stakes and withdrawals made were of a similar value. Analysis of the SARs identified differences in recorded personal details and several mentioned that documentation requested for customer due diligence (CDD) purposes was never provided. There appeared to be minimal cooperation between reporters.

So, what prompts the online gaming sector to disclose a SAR to the UKFIU?

- **Adverse media:** Forty-three of the 157 SARs were submitted following identification of media reports indicating that the subject was involved in criminality.
- **Losses:** Thirty-three of the SARs were submitted following a threshold amount being triggered over a specific time period ranging from 24 hours, seven days or 14 days, and one, three, eight or 12 months.
- **Documentation refused or none provided:** Thirty-two subjects were reported for failing to provide CDD and enhanced due diligence documentation. This was usually in addition to one of the above reasons.
- **Stolen to fund a gambling habit:** Twenty-five of the SARs disclosed a person who had stolen funds from an employer to fund a gambling habit. However, the figures provided did not necessarily corroborate this. In total, the SARs suggested that employees stole approximately 1.9 million pounds ($2.5 million) of which 379,000 pounds ($495,258) was gambled online. Nine further SARs suggested suspicion that the subject may be stealing funds from their employer to fund their online gambling.
- **Stolen cards:** Twelve of the SARs were related to gambled funds that originated from stolen bank cards or deposits made with third-party cards.

THIRTY-TWO SUBJECTS WERE REPORTED FOR FAILING TO PROVIDE CDD AND ENHANCED DUE DILIGENCE DOCUMENTATION

- **Mule accounts and third parties:** Nine of the SARs referenced accounts funded by third parties purely for online gambling purposes. There was no other account activity—such as bill payments, personal spending, and salary or benefit payments—suggesting the accounts were controlled by persons unknown.
- **Linked devices:** Nine reports mentioned subjects who gambled from linked devices associated with subjects previously reported for suspected money laundering offenses, suggesting these accounts might be controlled by unknown persons.
- **LEA inquiries:** Nine reports were submitted following LEA inquiries indicating the person was subject to a criminal investigation. This is in effect the SARs system working in reverse and these SARs are of little if any value to LEAs.
- **Nurses/caregivers:** Six SARs reported subjects in the nursing profession who stole from vulnerable victims in their care and used the funds for online gambling. These ranged from defrauding a victim of 101,000 pounds ($131,982) that was all gambled online to another stealing 13,000 pounds ($16,988) from an elderly patient who gambled only 160 pounds ($209) of this amount.
- **Fraudulent documents:** Three reports were made because of the receipt of suspected or confirmed fraudulent documentation.

Criminal exploitation of the online gaming sector

The 157 SARs identified 89 individuals known to the Police National Computer (PNC), a law enforcement database that contains the details of all persons arrested, convicted, cautioned or charged with a criminal offense. From this pool of 89 individuals:

- Seventy-six were men, while 13 were women.
- Ten were career criminals with approximately 250 criminal convictions between them. Most were known for violence and supplying controlled drugs. Two had previous convictions for money laundering, one of whom was reported for depositing 245,000 pounds ($320,152) and withdrawing 201,000 pounds ($262,656). Another with no money laundering convictions deposited 299,000 pounds ($390,718) and withdrew 288,000 pounds ($376,344), suggesting clear involvement in the laundering of criminal funds. Three were reported for triggering loss thresholds. The remainder were reported for providing suspected fraudulent documentation, LEA inquiries or adverse media. Only two had more than one SAR filed against their name with one having 13 and the other five.
- Only two of these 10 prolific offenders had an occupation shown, all except for one were men and the majority reside in the Yorkshire area.
- In total, those known to the PNC with criminal convictions deposited approximately 3.2 million pounds ($4.2 million), losing 620,000 pounds ($810,185) and withdrawing just under 1.7 million pounds ($2.2 million). (Compare that to those with

no criminal record who deposited approximately 1.5 million pounds [$1.9 million], lost 945,000 pounds [$1.2 million] and withdrew 235,000 pounds [$307,086].)

- Those with a criminal record resided in 27 English counties, the majority coming from London (14), Essex and Yorkshire (nine), Kent (six), no address shown (five), and Hertfordshire and Staffordshire (three).
- Dates of birth ranged from 1949 to 1998 with the majority (35) born in the 1980s of which 14 were born in 1988 or 1989.

These figures must be interpreted with caution as not all SARs provided indications of deposits, losses incurred or withdrawals made.

Women reported

Thirty-one women were reported who resided in Scotland, Wales and 13 different English Home Counties. The majority came from London followed by Cambridgeshire, Essex and Kent.

Their dates of birth ranged from 1954 to 2000. The majority were born in the 1970s and 1980s with the most frequent year being 1979.

Occupations included analyst, cleaner, consultant, director, sales and telecommunications. Six were listed as caregivers, all of whom were indicated to have stolen from vulnerable persons in their care by adverse media. Three were unemployed and two were students. Ten had no occupation shown. Thirteen of these women were known to the PNC, with the majority known for employee theft and fraud to fund their gambling addictions.

They were reported for the following:

- **Adverse media:** Stole from their employer or vulnerable victim in their care to fund gambling addiction.
- **LEA inquiries:** The subject was a suspect in a police investigation.
- **Losses:** Amounts lost ranged from 25,000 pounds ($32,669) to 659,000 pounds ($861,148).
- **Mule accounts:** The account used purely for gambling was funded by third parties.
- **Shared Internet Protocol (IP) address:** An IP address was shared with others previously reported for suspicion of money laundering

FORTY-THREE OF THE 157 SARS WERE DAML SARS, PREVIOUSLY KNOWN AS CONSENT SARS

DAML SARs

Forty-three of the 157 SARs were DAML SARs, previously known as consent SARs. This is a process whereby a reporter who suspects that they are dealing with the proceeds of crime seeks authority from the UKFIU to complete a transaction. If provided, it would negate any potential future prosecution for committing a prohibited money laundering offense. In most cases, a DAML should only be refused when positive police action in relation to the suspected illicit funds is likely to follow or is already under way.

Accordingly, DAML requests should trigger more money laundering investigations. Consequently, LEAs expend significant resources in responding to these disclosures.

If a defense is granted, the UKFIU makes it clear to reporters that this does not imply UKFIU approval of the proposed act; that it should not be taken as a statement that the property in question does or does not represent criminal property; and that it does not absolve them of their professional duties of conduct or regulatory requirements.

The 43 DAMLs were disseminated to 17 LEAs, based on the subject's postcode, to assess and make recommendations.

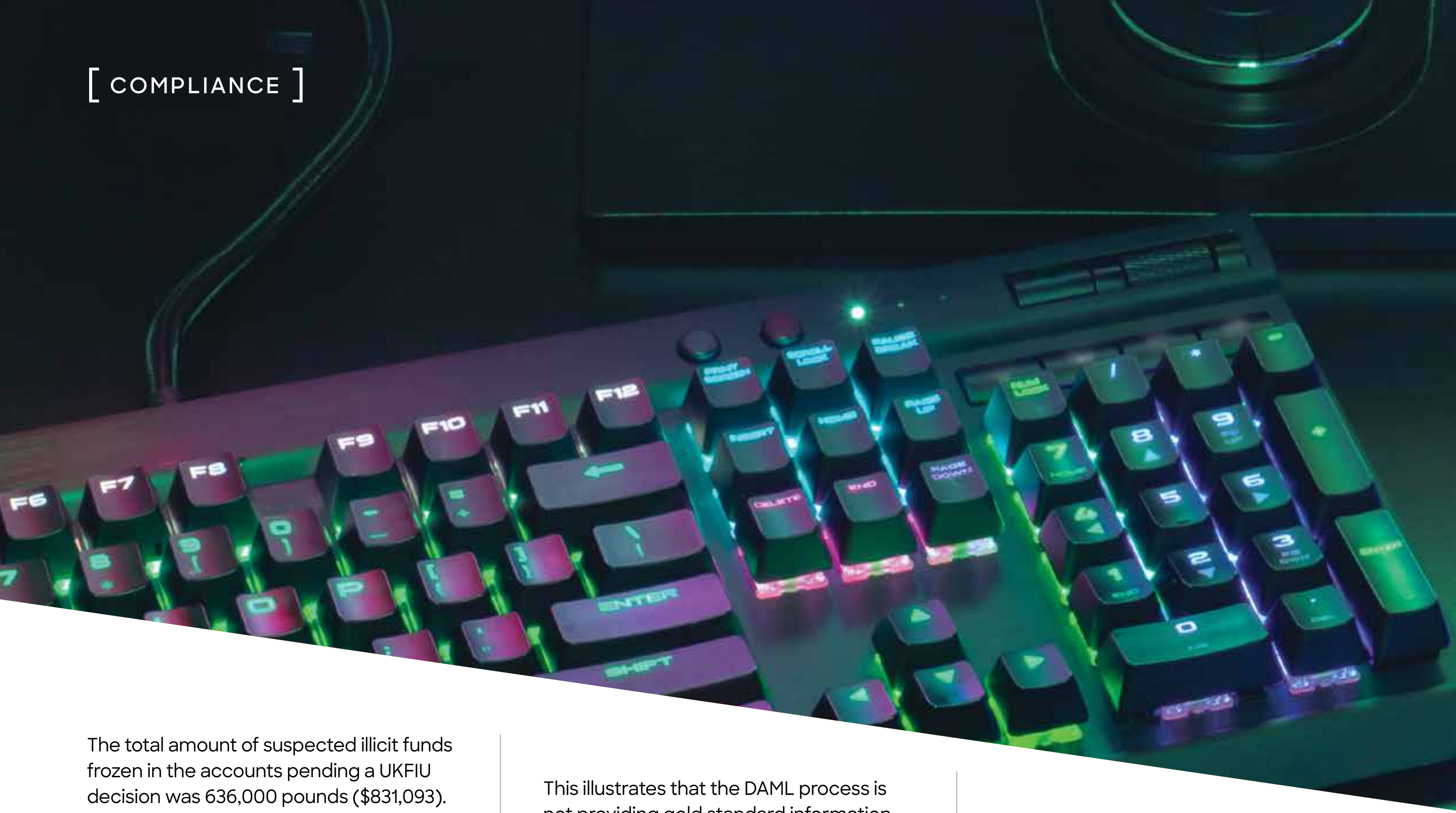
Eighteen went to the MPS; three to Essex and Cambridgeshire; two to West Yorkshire, West Mercia, West Midlands, Hampshire and Sussex; and one to Avon and Somerset, Cumbria, Devon and Cornwall, Durham, Dyfed-Powys, Hertfordshire, Norfolk, Nottinghamshire and Thames Valley.

The DAMLs identified 43 individuals (35 men, eight women), 20 of which (18 men, two women) had a criminal record. Twenty were subject of no other SAR, while 23 were subject to a further 115 SARs collectively.

Two of the DAMLs (made by the same operator) were incorrectly reported as the operator was not requesting a defense to carry out a prohibited money laundering offense. It is inconclusive whether this demonstrates an error in reporting or misunderstanding the DAML process.

Online gaming operators submitted DAMLs for the following reasons:

- Concern that the subject named in the DAML was not in charge or in control of the account
- Customer profile failed to align with recent account activity
- Customer failed to engage in the source of funds/source of wealth process
- Adverse media reports concerning winners and losers (Interestedly, one DAML was to pay back the stake only and did not include the winning amount!)



The total amount of suspected illicit funds frozen in the accounts pending a UKFIU decision was 636,000 pounds ($831,093). Initially, 2.5 million pounds ($3.3 million) were deposited into these accounts. These DAML amounts varied from 1.60 pence ($2.10) to 203,116 pounds ($265,422).

Ten DAML SARs were for 55 pounds ($72) or less and totaled 189 pounds ($247). Initially, 292,304 pounds ($381,968) were deposited into these online accounts. It is unlikely LEAs will deploy resources to recover such low sums as this would be both wasteful and disproportionate.

Three of the 43 DAML SARs had consent refused and just one generated the seizure of illicit funds (11,200 pounds [$14,636], under 2% of the reported amount).

The evaluation indicated that non-DAML SARs might appear more worthy of LEA investigation. Most notably, SARs were filed suggesting that a subject might be misappropriating company funds to gamble. Those reported are usually working in positions of trust and sums deposited are considerable and not commensurate with their salaries. Therefore, LEAs are denied the opportunity to restrain, freeze and seize potential illicit assets.

This illustrates that the DAML process is not providing gold standard information of criminality and might be misunderstood by many online reporters.

Conclusion

The analysis clearly illustrates the depth of criminal use of the U.K.'s online gaming industry. It confirms that online gambling appears to offer a low-cost opportunity to launder criminal funds. It also questions previous reports suggesting that a significant proportion of the money laundering that occurs within the industry is by criminals spending the proceeds of crime for leisure rather than "washing" criminal funds.

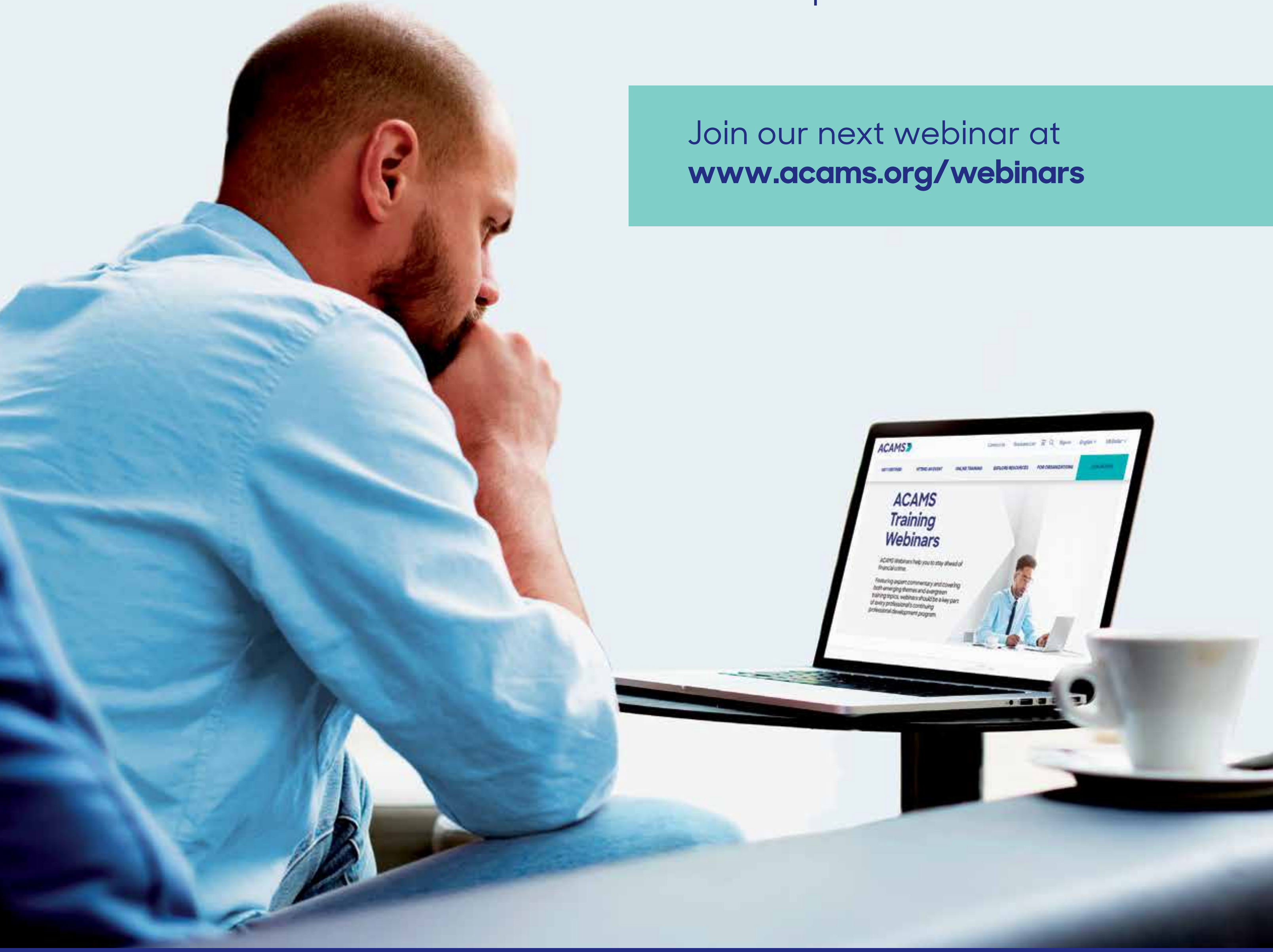
The analysis suggests that U.K. online gambling operators have insufficient knowledge of their customers reducing their ability to conduct affordability assessments. This prohibits early intervention to identify problem gamblers, prevent them from being drawn into criminality to fund their gambling lifestyle, and allow them to gamble well in excess of what their profile would have suggested was affordable. Consequently, operators are less likely to prevent harm from gambling and deter, prevent and detect criminal activity.

This lack of customer knowledge suggests that that operators are failing to understand their risks and questions whether operators are doing enough to prevent money laundering and other financial crime. Thus, this information might require institutions to re-evaluate their AML/CTF programs, risk appetite and customer acceptance policy.

Graham Edwards, CAMS, accredited financial investigator, Metropolitan Police Service, London, U.K., Graham.edwards3@met.police.uk

[1] Gross gambling yield is the amount retained by operators after the payment of winnings but before the deduction of the costs of the operation.

[2] Source of funds concerns the provenance of the funds of the customer and how the funds being deposited with the operator were generated. Source of wealth concerns the origins of the customer's entire wealth.These terms are mentioned as preventive measures in the Financial Action Task Force's Recommendations 10 and 12 as clarity concerning the legitimacy of a customer's source of funds/source of wealth significantly reduces the risk of money laundering.



ACAMS

Venezuela–Blink and you may miss it

The COVID-19 pandemic has exposed the best and worst of what governments can do for their citizens. Some nations' leaders and governmental systems have worked to ensure that the least among their populace can generally survive and (hopefully) thrive with some assistance; others have proven inadequate as long ignored systemic deficiencies have been exposed. Even worse, some leaders have taken advantage of the crisis to extend their power and exploit national resources, with catastrophic results. Moreover, prior to the COVID-19 outbreak, a number of countries around the world were experiencing civil unrest and social upheaval was already evident, resulting in similarly grave outcomes. One such country is Venezuela.

According to Transparency International's 2019 Corruption Perception Index, Venezuela now ranks among the most corrupt countries in the world, joining Sudan, Libya, Somalia, North Korea and Afghanistan, among others.[1] To say that Venezuela has undergone a precipitous decline over the last 20 years would be an understatement. Venezuela was once a generally stable and developing country with a solid middle class, vast natural resources, a robust tourism industry and potential for economic growth. Now, over the course of two successive presidential administrations—first Hugo Chavez and later his successor, Nicolas Maduro—the country has been turned upside down, with Maduro now metaphorically shaking the money out of its very pockets.[2] The Venezuelan leader's rule resembles that seen in countries such as Zimbabwe. To the casual observer, the collapse of Venezuela and other nations under harsh governmental regimes could be viewed as the predicable consequence tied to the actions of dictators. However, anti-money laundering (AML) professionals are not casual observers; they know the patterns and practices that permit such systemic looting and warrant further analysis.

The kleptocrat's financial playbook

Merriam-Webster's dictionary defines a kleptocracy as a "government by those who seek chiefly status and personal gain at the expense of the governed."[3] There have been numerous governments worldwide and throughout history that have fit this definition. However, despite the global recognition of the destruction created by modern kleptocracies, such regimes seem particularly adept at stealing their nation's wealth in the 21st century. Venezuela's recent decline is highly notable, not only for the dramatic extent of citizens' suffering, but also for the speed and means by which its corrupt leaders managed to expropriate the state's treasury unabated. The country's collapse has seemingly been enabled through the application of a kleptocratic "financial playbook," with international money laundering serving as a principal tool used to capture and exploit a nation's wealth. Certainly, many rulers and authoritarians have looted their countries' wealth; however, kleptocrats seemingly take governing by force to another level. Brutal domination of the masses and warmongering is fine to them, but their primary goal of gaining and maintaining power is to get, and remain, rich. As with any criminal enterprise, once obtained, this newfound wealth must be "sanitized" in order to maintain an air of legitimacy. Consider the following stages of kleptocratic actions and their correlation with the three stages of money laundering.

Step one: Capture the state (placement stage)

Some "traditional" dictators claimed power over the state, nationalized resources, and maintained a veneer of governing while skimming a bit of the state's wealth (e.g., Iran, Cuba, Indonesia, or Venezuela under Chavez); kleptocrats, however, seem more distinct in their approach to managing state resources. Kleptocrats seem to prefer privatization, as they go about selling off state assets. In doing so, they may claim direct ownership, ownership interest, or payments through their sale to other parties (e.g., family and cronies). First, kleptocrats aggressively seek to bring the courts, legislature, judiciary, institutions of society and media under their control. It helps to keep the military on their side (and under payroll) to avoid being overthrown. Once completed, kleptocrats will ensure the open sale of state resources, which eventually leads to contracts over which they can exert "anonymous" control. Privatization also facilitates the "legal" veneer of business activity, while creating opportunities for expropriation of state wealth. With kleptocrats having consolidated the power of the state and resources of the legislature through the government itself, the foundation is set for looting to begin.

Step two: Employ professional intermediaries (placement stage)

As extensively covered by the "Panama Papers,"[4] a long-time tool of the wealthy has been the use of offshore agent

services offered by firms such as Mossack Fonseca to establish accounts in tax-lenient nations with casual banking regulations. Whether for legitimate or criminal profits, the end goal is to evade the prying eyes of tax authorities and law enforcement. Lawyers, accountants and offshore financial services providers serve several key purposes here:

- First, they facilitate the establishment of an additional buffer for the corrupt head of state through anonymous corporate vehicles—a must-have for large-scale money laundering. These shell companies also create a plausible deniability buffer toward any outward association with corrupt activities that may occur.
- Second, professional intermediaries activate the offshore network that will allow for efficient movement and distribution of looted state funds.
- Third, they enable ready access to the keystone of the international money laundering machine: offshore financial institutions (FIs) with weak AML and sanctions controls and/or management willing to service illicit funds presented to them by wealthy clientele.

Step three: Employ personal intermediaries (layering stage)

Once settled into power, kleptocrats facilitate the sale of state resources and extraction rights to family, friends, cronies and enablers (e.g., cabinet members, legislature and the military) using the pre-established network of shell companies. This can ensure entrenchment of authority over the government and help diminish the risk of overthrow. The recent exposé of Isabel dos Santos, daughter of former Angolan president José Eduardo dos Santos, and the case of Teodorin Obiang of Equitorial Guinea evidence the shadowy application of this step.[5]

Step four: Keep (potential) local enemies close and leverage them (layering and integration stages)

Kleptocrats will conscript additional intermediary resources hostile to the government and its citizens whose own illicit activities can facilitate state-run criminal exploitation. Under threat of unleashing the state's military and law enforcement resources, kleptocrats can co-opt the services of criminal networks to serve their needs. Such was the case in Panama under the regime of Manuel Noriega, a head-of-state turned narcotics trafficker.[6] Venezuela shares a large border with Colombia, and black-market smuggling and narcotics trafficking networks have provided the Maduro regime ready access to the criminal underground. First, exploitation of these channels provides Maduro an illicit revenue stream and ability to leverage professional money laundering expertise to facilitate moving funds offshore.[7] Second, Maduro has efficiently applied both "traditional" (e.g., illicit foreign currency exchange) and, more recently, nontraditional (e.g., virtual assets)[8] criminal techniques to launder stolen state funds. Getting familiar with cutting-edge money laundering services used by traffickers can help kleptocrats refine the methods used to layer and integrate their illicit funds.

Step five: Maintain (now fewer) international allies—and leverage them as well (layering and integration stages)

With deeper ties to Russia in recent years, Maduro would seem to have developed access to both the power structure and advisory resources of what could arguably be the largest, most effective kleptocratic regime in modern history. By maintaining diplomatic and economic ties to the Kremlin as well autocratic regimes such as Iran and Cuba, Maduro can facilitate financial and trade agreements to ensure sanctions avoidance and continued access to capital.

International investigative journalists with the Organized Crime and Corruption Project (OCCRP) have exposed several large-scale money "laundromats" in Europe in recent years where paths cross between organized crime, government officials and the financial sector to facilitate high volume money laundering.[9] Such organized schemes, whether independent operations or sanctioned by the state itself, generally do not occur without the knowledge of state leadership. Furthermore, when applied successfully, the preceding steps can also enable the evasion of economic sanctions restrictions and embargoes applied by hostile foreign governments. A recent *ABC News* article points to the means by which Maduro has continued to export Venezuelan oil to skirt U.S. sanctions.[10] As demonstrated by a "rogue's gallery" of predecessors including Augusto Pinochet, Idi Amin, François "Papa Doc" Duvalier, Kemusu "Suharto" Argamulja and many others during the mid-to-late 20th century, the aforementioned principles can be highly effective to achieve "state-sponsored" personal wealth.

Where is the people's money?

A number of international penalties have been leveraged against the Maduro regime in recent years in the form of pressure through economic sanctions against its leaders and assets, led primarily by the U.S. government. In addition to various U.S. sanctions against Maduro and his associates, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued an updated advisory for FIs on corruption in Venezuela (FIN 2019-A002).[11] The advisory provides a highly detailed account of major laundering schemes, indicted individuals and red flags to alert of possible suspicious transactions and activities associated with Maduro and his cohorts. Despite such actions, Maduro has continued to employ resources to hoard personal wealth through offshore vehicles while extending his rule. Several recent key cases and arrests may have revealed some of the secrets behind how his regime has maintained its grip on draining the country's treasury. Some incidents have ties to the Miami, Florida region, noteworthy not only for its Venezuelan expatriate population, but also as a long-time U.S. destination of choice for illicit fund flows from Latin America.

- In late 2019, University of Miami professor Bruce Bagley, a renowned expert on Latin American organized crime and money laundering, was arrested by the FBI for helping launder $3 million in dirty money from Venezuela. It was alleged that "Bagley began using his expertise to funnel money 'believed to be derived from graft and corruption in connection with public works projects in Venezuela' into the United States."[12]
- In April 2020, South Florida federal authorities seized $450 million in "bank accounts—luxury properties, show horses, high-end watches and a super-yacht" owned by more than a dozen government officials and business people in Venezuela. This seizure included assets owned by Alejandro Andrade, Venezuela's former national treasurer, who is currently serving a 10-year sentence in a U.S. prison on corruption and money laundering charges.[13]

Maduro has continued to employ resources to hoard personal wealth through offshore vehicles while extending his rule

- On June 2, 2020, per the aforementioned currency fraud, Joselit Ramirez Camacho, head of Venezuela's cryptocurrency initiative, became wanted by the U.S. government on charges of corruption and links to the narcotics trade. He has also been indicted in the Southern District of New York on charges related to sanctions violations. A $5 million bounty has been offered for information leading to his arrest.[14]
- In June 2020, U.S. authorities indicted Alex Saab, a Colombian businessman, as the chief money launderer for Maduro's regime. Saab was captured under an Interpol "Red Notice" and detained while en route from Caracas, Venezuela to Iran on the island of Cape Verde off the West African coast. Saab is accused of being the front man for a vast network of money laundering and corruption in Venezuela through shell companies in the United Arab Emirates, Turkey, Hong Kong, Panama, Colombia and Mexico. In addition, in July 2019, the U.S. Department of Justice (DOJ) indicted Saab and another businessman for bribing Venezuelan officials and diverting some $350 million to overseas accounts. Additional wealth transfer schemes involving Maduro family members and associates have been tied to Saab.[15]
- On July 8, 2020, Venezuelan businessman and former Maduro official Raúl Gorrín—previously indicted by the DOJ in November 2018 for a money laundering conspiracy involving over $1 billion in bribes[16]—was alleged to be behind a scheme to smuggle 81 luxury

vehicles through the Port Everglades to Venezuela. U.S. Homeland Security Investigations stated that the vehicles had been bought through a "...network of straw buyers and shell companies in South Florida... for use by the wealthy, the politically connected and the police."[17] Gorrín is a billionaire listed on the Immigration and Customs Enforcement's Most Wanted list[18] on charges of money laundering and has been labeled in some circles as the "biggest money launderer in the world." He remains at large.

Summary

It is understood that all empires and nations have experienced upheaval of some sort at some point, whether through willful or uncontrollable changes in government and social order. Some may fall slowly, others swiftly and seemingly without notice at the hands of kleptocratic regimes. Chavez created a cult of personality during his time in office in Venezuela and Maduro is noted for growing in stature under his tutelage. Elections held after Chavez's death in 2013 unfortunately presented citizens the option to vote to retain the "familiar." The result was Maduro, notwithstanding the fact that suspicious efforts surround those initial and subsequent elections. Maduro was once named "2016 Man of the Year in Organized Crime and Corruption" by the OCCRP.[19] Time will tell if he becomes a two-time winner like his Russian counterpart Russian President Vladimir Putin.

Brian Arrington, MBA, CAMS, communications director of the ACAMS Chicago Chapter; managing director, US AML Compliance, CIBC Bank USA, Chicago, IL, USA, brian.arrington@cibc.com

The views and opinions expressed are those of the author and do not necessarily represent the views and directives of CIBC Bank USA.

Recommended additional reading: "The Oil Curse: How Petroleum Wealth Shapes the Development of Nations," by Michael L. Ross.

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

[2] "Nicolás Maduro: Corruption and Chaos in Venezuela," *U.S. Department of State*, August 6, 2019, https://www.state.gov/nicolas-maduro-corruption-and-chaos-in-venezuela-2/

[3] "kleptocracy," *Merriam-Webster Dictionary*, https://www.merriam-webster.com/dictionary/kleptocracy

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

[5] "Isabel dos Santos: President's Daughter Who Became Africa's Richest Woman," *The Guardian*, January 19, 2020, https://www.theguardian.com/world/2020/jan/19/isabel-dos-santos-president-daughter-africa-richest-woman-angola; "Global Witness Welcomes Historic Ruling Against Teodorin Obiang," *Global Witness*, October 27, 2017, https://www.globalwitness.org/en/press-releases/global-witness-welcomes-historic-ruling-against-obiang-fight-against-corruption/

[6] Elida Moreno, "Panama's Noriega: CIA spy turned drug-running dictator," *Reuters*, May 30, 2017, https://www.reuters.com/article/us-panama-noriega-obituary-idUSKBN18Q0NW

[7] Nick Paton Walsh, Natalie Gallón and Diana Castrillon, "Corruption in Venezuela has created a cocaine superhighway to the US," *CNN*, April 17, 2019, https://www.cnn.com/2019/04/17/americas/venezuela-drug-cocaine-trafficking-intl/index.html

[8] "Treasury Targets Venezuela Currency Exchange Network Scheme Generating Billions of Dollars for Corrupt Regime Insiders," *U.S. Department of the Treasury*, January 8, 2019, https://home.treasury.gov/news/pressreleases/sm583; Paddy Baker, "US Offers $5M Bounty for Arrest of Venezuela's Crypto Chief," *Yahoo Finance*, June 2, 2020, https://finance.yahoo.com/news/us-offers-5m-bounty-arrest-145639026.html

[9] "The Real-Life Laundromats," *Organized Crime and Corruption Reporting Protocol*, https://www.occrp.org/en/laundromats/

[10] Joshua Goodman, "Venezuela sanctions set off fight for 'plundered' oil cargo," *ABC News*, June 30, 2020, https://abcnews.go.com/US/wireStory/venezuela-sanctions-set-off-fight-plundered-oil-cargo-71529069

[11] "Updated Advisory on Widespread Public Corruption in Venezuela," *Financial Crimes Enforcement Network*, May 9, 2019, https://www.fincen.gov/sites/default/files/advisory/2019-05-03/Venezuela%20Advisory%20FINAL%20508.pdf

[12] "He was the go-to expert on money laundering. Now he's been charged with laundering money," *The Washington Post*, November 19, 2019, https://www.washingtonpost.com/nation/2019/11/19/bruce-bagley-money-laundering-university-miami-expert/

[13] "Miami Feds Seize $450 Million – Cash, Condos, Horses – in Venezuelan Corruption Cases," *Yahoo News*, April 28, 2020, https://www.yahoonewsz.com/coronavirus/miami-feds-seize-450-million/

[14] "De La Trinidad Ramirez Camacho, Joselit," *U.S. Immigration and Customs Enforcement*, https://www.ice.gov/most-wanted/de-la-trinidad-ramirez-camacho-joselit

[15] "U.S.-Indicted Dealmaker for Venezuela's Maduro Detained on Way To Iran," *Radio Free Europe*, June 14, 2020, https://www.rferl.org/a/maduro-venezuela-money-laundering-iran-/30669592.html; "U.S.-Indicted Dealmaker for Venezuela's Maduro Detained on Way To Iran," *Anti-Corruption Digest*, June 15, 2020, https://anticorruptiondigest.com/2020/06/15/u-s-indicted-dealmaker-for-venezuelas-maduro-detained-on-way-to-iran/#axzz6U4W3iwBV

[16] "Venezuelan Billionaire News Network Owner, Former Venezuelan National Treasurer and Former Owner of Dominican Republic Bank Charged in Money Laundering Conspiracy Involving Over $1 Billion in Bribes," *U.S. Department of Justice*, November 20, 2018, https://www.justice.gov/opa/pr/venezuelan-billionaire-news-network-owner-former-venezuelan-national-treasurer-and-former

[17] Chris Dalby, "Venezuelan Money Laundering Schemes Continue To Thrive in US," *InSight Crime*, July 13, 2020, https://www.insightcrime.org/news/analysis/venezuelan-money-laundering-schemes-continue-to-thrive-in-us/

[18] "Venezuelan attorney and businessman added to ICE Most Wanted List for conspiracy to violate the Foreign Corrupt Practices Act and money laundering," *U.S. Immigration and Customs Enforcement*, January 15, 2020, https://www.ice.gov/news/releases/venezuelan-attorney-and-businessman-added-ice-most-wanted-list-conspiracy-violate

[19] "Person of the Year 2016: Nicolás Maduro," *Organized Crime and Corruption Reporting Project*, https://www.occrp.org/en/poy/2016/

Georgian President Mikheil Saakashvili's fight against corruption

Georgia is a small country in the South Caucasus. In the hills of Tbilisi, a statue of Kartlis Deda (Mother Georgia), stands vigilant, holding a sword to deter foes and a bowl of wine to welcome friends.

Unfortunately, Kartlis Deda was unable to defend Georgia from war, rampant corruption, crime and separatist conflict between 1992 and 2003. By the time President Eduard Shevardnadze resigned, Georgia was 124th out 133 on Transparency International's Corruption Perceptions Index. Yet 10 years later, Georgia substantially reduced corruption, developed its economy and became a functional democracy, rising to 55th out of 177, which is comparable to multiple European Union countries.[1]

Georgia declared independence in 1991 and elected nationalist President Zviad Gamsakhurdia in a landslide.[2] Gamsakhurdia was abruptly ousted via a putsch in January 1992 and Georgia descended into civil war. The autonomous regions of South Ossetia and Abkhazia effectively, albeit unofficially, broke away.[3] Gamsakhurdia failed to win back control of the country and allegedly committed suicide in December 1993.

Georgia's civil war ended in 1995 and victorious interim leader Shevardnadze was elected president in a wave of optimism. Shevardnadze previously served as first secretary of the Communist Party of Georgia from 1972 to 1985, and then as Minister of Foreign Affairs under Mikhail Gorbachev.[4] As first secretary, his economic reforms were largely successful, bringing a degree of liberalization to the Georgian Soviet Socialist Republic and avoiding economic stagnation.[5]

Shevardnadze's presidency was far less effective and he struggled to bring stability to Georgia.[6] His previous economic reforms were rendered obsolete. Although the president himself was never charged with corruption, several members of his family and his administration who had become visibly wealthy in a poor country were charged. Georgians’ patience with Shevardnadze dissolved quickly after his reelection.[7]

Shevardnadze’s downfall came in November 2003 as Georgians elected a new Parliament. Official results suggested victory for Shevardnadze’s allies, but exit polls directly contradicted official results and protests broke out amid allegations of ballot-box stuffing and electoral violence.[8] Protests grew larger and louder when Organization for Security and Co-operation in Europe representatives denounced the election.[9] President Shevardnadze resigned and the nonviolent movement to oust him was named the Rose Revolution.

After Shevardnadze resigned, Mikheil Saakashvili—a prominent opposition leader and former member of Parliament who had resigned in protest years earlier—was elected president. The United National Movement (UNM), the party he founded, breezed to victory in the parliamentary election two months later.[10]

Saakashvili’s reforms

Saakashvili quickly set out to enact both symbolic and structural reform, giving Georgia a new flag and national anthem as well as starting an extensive anti-corruption project. “In 2004, Georgia made the biggest leap of any country in terms of its perception of corruption, with 60 per cent of respondents expecting corruption levels to decrease over the next three years.”[11] President Saakashvili’s anti-corruption drive focused primarily on “police, tax administration, customs, public services and education.”[12]

Georgia’s police force was feared, distrusted and disastrously corrupt. President Saakashvili said, “…We had one of the most corrupt police forces…. Not only do you have to take bribes from the people but you also have to share part of your corrupt income with your superiors… with the government that appointed you.”[13]

Georgia, much like its regional neighbors, has struggled with the influence of oligarchs in politics and government

In 2005, President Saakashvili fired the entire 30,000-strong police force and enlisted the U.S. to help recruit new officers.[14] Saakashvili increased salaries to discourage previously rampant bribery and drive recruitment. Georgia’s police force was quickly rebuilt on stronger foundations. The new force quickly earned the Georgian people’s trust and Georgians became willing to call the police.[15] Before 2005, Georgia’s police force was a symbol of dysfunction and corruption. But their rapid, effective reform demonstrated that deep-rooted problems could be rectified.

Low-level corruption in Georgia prior to the Saakashvili administration was broad and extended into the public sector. Georgia was a poor country rife with crime, where bribes were taken just to survive. Thus, Saakashvili gave public servants a considerable raise. “Under Shevarnadze, state salaries were so small as to be symbolic, and public servants and policemen had to use their position to obtain money by other means,” said Ghia Nodia, a Georgian political analyst.[16] Higher salaries created public sector stability and the Georgian government started functioning more effectively, providing citizens with public services free of corruption.[17] By 2013, Transparency International noted that only 4% of Georgian survey respondents reported paying a bribe for public services.[18]

Georgia, much like its regional neighbors, has struggled with the influence of oligarchs in politics and government. President Saakashvili held the oligarchs who flourished under the Shevardnadze administration accountable, having many of them arrested with most agreeing to plea bargains.[19]

To further attack corruption, President Saakashvili began to address tax collection. Under Shevardnadze, tax revenue was meager, despite high tax rates, and tax evasion was rampant.[20] While President Saakashvili did not universally dismiss tax collectors like he did to the police force, his clampdown was similarly emphatic and sweeping.

> “Harsh sentences given to tax inspectors on corruption charges were combined with widely broadcast arrests of corrupt officials, and quickly discouraged most of them from taking bribes. Authorities arrested numerous former officials and businessmen suspected of corruption. They were given an option of buying themselves out of prison by paying substantial amounts of money to the treasury.”[21]

Saakashvili’s tactics were condemned as heavy-handed and authoritarian, but the message was clear. The highly public crackdown on tax evasion was followed by extensive, “three-pronged” tax code simplification—specifically reducing tax rates, broadening the tax base and improving tax administration.[22] After the tax code overhaul, Saakashvili’s administration cut rates to attract foreign investment and encourage economic growth, while newly secured revenue streams bolstered the budget and enabled the Georgian government to embark on extensive spending projects to improve infrastructure.[23] President Saakashvili simultaneously raised tax revenue and reduced tax rates, "The social security contribution changed the most, from 33 to 20%. The corporate income tax rate was decreased from 20% to 15%, and…the dividend and interest tax rate was reduced from 15% to 5%. The state budget saw a nearly 300% increase."[24]

In addition, President Saakashvili removed barriers to doing business in Georgia. His anti-corruption initiatives were often accompanied by extensive privatization. Georgia was hobbled by a bloated, state-dominated economy; its private sector accounts for only 40% of total employment, compared to 75% in Armenia and 80% in Estonia.[25] Under the Saakashvili administration, foreign investment grew rapidly and the country won acclaim from the World Bank for its extensive reforms in 2006 and 2008.[26] Georgia vastly improved its standing in the World Bank's "Doing Business Report," rising from 112th place in 2005 to 11th place in 2010. The number of registered companies in Georgia rose to 51,000 in 2007 from 36,000 in 2005.[27]

President Saakashvili also overhauled Georgia's education infrastructure in his anti-corruption effort. His administration shuffled university leadership and moved the admissions process away from university bureaucracy by instituting a country-wide examination system and revised accreditation procedures. Under President Shevardnadze, bribery was rampant, even necessary at Georgian universities, just to secure admission.[28] Saakashvili greatly improved transparency and accountability, and confidence in the country's Ministry of Education grew quickly and remains high today.[29]

Saakashvili's shortcomings

Despite Saakashvili's success in fighting corruption, he was a polarizing leader.[30] Large, sometimes violent street protests against him were common.[31] The same police force Saakashvili reformed worked under a judicial system many Georgians considered excessively heavy-handed.[32] Of the justice system, Thomas de Waal, a South Caucasus expert at the Carnegie Center in Washington, said, "…torture became absolutely routine." There were also almost zero acquittal cases in criminal trials, mass surveillance and telephone tapping. In addition, a lot of pressure was put on businessmen so they would contribute to government projects.[33] Georgia's prisoner population soared under President Saakashvili, and in 2012 a video of prison guards torturing inmates led to the resignation of the minister of correction, probation and legal assistance.[34]

Other critiques of Saakashvili include primary and secondary education lagging behind, despite educational reform significantly improving Georgia's universities.[35] In addition, Saakashvili's economic reforms did not significantly reduce poverty and unemployment despite soaring economic growth.[36] Finally, President Saakashvili's leadership style was often considered authoritarian, despite his role in the Rose Revolution.

After Saakashvili

Saakashvili faced term limits as president so he stepped down in 2013. His UNM party was soundly defeated in the 2012 parliamentary election by Georgian Dream, a big-tent, center-left coalition, and the UNM's presidential nominee in 2013 suffered a similarly decisive defeat.[37] Georgia's rejection of the UNM sobered the outgoing Saakashvili and he acknowledged flaws in his presidential administration. In his 2013 farewell speech, Saakashvili said he was aware that some of his reforms had come at "a very high cost" and extended his sympathy to all those who felt wronged by his radical methods.[38]

Today, Georgia is a relatively stable parliamentary republic grappling with lingering, though significantly reduced, corruption. Despite Saakashvili's elimination of most low-level corruption, oversight in Georgia's government is often insufficient and its system of checks and balances remains lopsided. According to Transparency International, "Entrenched corruption, strong patronage networks, and a lack of clear separation between private enterprise and public office significantly challenge democracy and good governance in Georgia."[39] President Saakashvili's privatization drive successfully grew the Georgian economy but lacked oversight. Government contracts see little competition and the country's communications commission has repeatedly been accused of selective enforcement of regulations.[40]

When President Saakashvili left office in 2013, he left Georgia in a stable position, but with room for improvement. His success came from political momentum, sweeping electoral mandates and an ability to build from the ground up. Saakashvili inherited a country on the brink of disaster and rode into power on a wave of momentum driven by nonviolent revolution. It is rare that newly elected heads of state come to power with that magnitude of momentum, and it is possible Saakashvili was only able to enact such wide-reaching reforms because Georgia's institutions were weak and easy to tear down and rebuild. That does not diminish Saakashvili's accomplishments, but it does suggest that the reforms he enacted may not be so easily translatable to another country.

Nonetheless, Saakashvili provided a flawed but effective blueprint for anti-corruption reforms, albeit reform that depended on popular, nonviolent revolution to bring democracy.

Kyle Menyhert, graduate student, Schar School of Policy and Government, George Mason University, Alexandria, VA, USA, kylemenyhert@gmail.com

Today, Georgia is a relatively stable parliamentary republic grappling with lingering, though significantly reduced, corruption

[1] Nana Lobzhanidze, “Transparency International: Level of Perceived Corruption in Georgia Stable,” *Transparency International Georgia*, December 3, 2013, https://www.transparency.ge/en/content/stub-688 (accessed May 19, 2020).

[2] Martin McCauley, “Obituary: Zviad Gamsakhurdia,” *The Independent*, February 25, 1994, https://www.independent.co.uk/news/people/obituary-zviad-gamsakhurdia-1396384.html (accessed May 19, 2020).

[3] Ibid.

[4] William Courtney, Hon. Kenneth S. Yalowitz and Denis Corboy. “Remembering Eduard Shevardnadze,” *Wilson Center*, July 8, 2014, www.wilsoncenter.org/article/remembering-eduard-shevardnadze (accessed May 19, 2020).

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] “Georgia Parliamentary Elections, 2 November 2003,” *Organization for Security and Cooperation in Europe*, January 28, 2004, https://www.osce.org/files/f/documents/2/0/22205.pdf (accessed May 19, 2020).

[10] Claire Bigg, “Mikheil Saakashvili’s Polarizing Legacy,” *Radio Free Europe/Radio Liberty*, October 24, 2013, https://www.rferl.org/a/saakashvili-mixed-legacy/25146918.html (accessed May 19, 2020).

[11] Erekle Urushadze, “Overview of Corruption and Anti-Corruption in Georgia,” *Transparency International*, November 20, 2013, https://knowledgehub.transparency.org/helpdesk/overview-of-corruption-and-anti-corruption-in-georgia (retrieved May 19, 2020).

[12] Ibid.

[13] Robert Siegel, “Georgia’s National Police Corruption Project,” *National Public Radio*, September 15, 2005, https://www.npr.org/templates/story/story.php?storyId=4849472 (accessed May 19, 2020).

[14] Ibid.

[15] Ibid.

[16] Claire Bigg, “Mikheil Saakashvili’s Polarizing Legacy,” *Radio Free Europe/Radio Liberty*, October 24, 2013, https://www.rferl.org/a/saakashvili-mixed-legacy/25146918.html (accessed May 19, 2020).

[17] Ibid.

[18] Erekle Urushadze, “Overview of Corruption and Anti-Corruption in Georgia,” *Transparency International*, November 20, 2013, https://knowledgehub.transparency.org/helpdesk/overview-of-corruption-and-anti-corruption-in-georgia (accessed May 19, 2020).

[19] “The Political Economy of Georgia’s Transformation: Before and After the Rose Revolution,” *Young Initiative on Foreign Affairs and International Relations*, June 20, 2012, www.ifair.eu/2012/06/20/the-political-economy-of-georgias-transformation-before-and-after-the-rose-revolution/ (accessed May 19, 2020).

[20] Olena Bilan, “Tax Reform in Georgia: Lessons for Ukraine,” *VoxUkraine*, November 25, 2015, https://voxukraine.org/en/tax-reform-in-georgia-lessons-for-ukraine-en/ (accessed May 19, 2020).

[21] Ibid.

[22] “The Georgian Taxation System – An Overview,” *Transparency International Georgia*, May 2010, https://www.transparency.ge/sites/default/files/post_attachments/Taxation%20in%20Georgia%20_ENG_final_0.pdf (accessed May 19, 2020).

[23] Max Skubenko, “Tax Reform in Georgia: Lessons for Ukraine.”

[24] Ibid.

[25] John B. Taylor, “Economic Freedom and Georgia’s Rose Revolution.” *U.S. Department of the Treasury*, November 22, 2004, https://www.treasury.gov/press-center/press-releases/Pages/js2116.aspx (accessed May 19, 2020).

[26] “The Political Economy of Georgia’s Transformation: Before and After the Rose Revolution,” *Young Initiative on Foreign Affairs and International Relations*, June 20, 2012, www.ifair.eu/2012/06/20/the-political-economy-of-georgias-transformation-before-and-after-the-rose-revolution/ (accessed May 19, 2020).

[27] Ibid.

[28] Beka Tavartkiladze, “How Georgia Fought Academic Corruption,” *World Education News and Reviews*, December 8, 2017, https://wenr.wes.org/2017/12/how-georgia-fought-academic-corruption (accessed May 19, 2020).

[29] Ibid.

[30] Claire Bigg, “Mikheil Saakashvili’s Polarizing Legacy,” *Radio Free Europe/Radio Liberty*, October 24, 2013, https://www.rferl.org/a/saakashvili-mixed-legacy/25146918.html (accessed May 19, 2020).

[31] “The Political Economy of Georgia’s Transformation: Before and After the Rose Revolution,” *Young Initiative on Foreign Affairs and International Relations*, June 20, 2012, www.ifair.eu/2012/06/20/the-political-economy-of-georgias-transformation-before-and-after-the-rose-revolution/ (accessed May 19, 2020).

[32] Ibid.

[33] Claire Bigg, “Mikheil Saakashvili’s Polarizing Legacy,” *Radio Free Europe/Radio Liberty*, October 24, 2013, https://www.rferl.org/a/saakashvili-mixed-legacy/25146918.html (accessed May 19, 2020).

[34] Ibid.

[35] Ibid.

[36] “The Political Economy of Georgia’s Transformation: Before and After the Rose Revolution,” *Young Initiative on Foreign Affairs and International Relations*, June 20, 2012, www.ifair.eu/2012/06/20/the-political-economy-of-georgias-transformation-before-and-after-the-rose-revolution/ (accessed May 19, 2020).

[37] Claire Bigg, “Mikheil Saakashvili’s Polarizing Legacy,” *Radio Free Europe/Radio Liberty*, October 24, 2013, https://www.rferl.org/a/saakashvili-mixed-legacy/25146918.html (accessed May 19, 2020).

[38] Ibid.

[39] Erekle Urushadze, “Overview of Corruption and Anti-Corruption in Georgia,” *Transparency International*, November 20, 2013, https://knowledgehub.transparency.org/helpdesk/overview-of-corruption-and-anti-corruption-in-georgia (accessed May 19, 2020).

[40] Ibid.

Risky crypto remittances in the Philippines

Remittances are an essential part of the global economy, particularly in developing economies.[1] In the Philippines, overseas remittances formed 10.2% of the country's GDP in 2018.[2] Over 65% of the domestic population, made up of 109 million people, is unbanked.[3] Given the cliché in cryptocurrency[4] around the ability of digital assets to "bank the unbanked," it is not surprising that this industry has exploded in the Philippines. Tambunting Pawnshops[5] and 7-Eleven stores across the country have partnered with the U.S.-based app Abra to provide the next generation of financial services to Filipinos. Abra claims to provide access to over 150 countries[6] and 85 cryptocurrencies,[7] with intentions to expand in the future. However, the regulatory environment in the Philippines raises concerns that the platform may be used for illegal activity such as money laundering and terrorist financing. The level of domestic terrorism and concerns about extrajudicial killings[8] has led to the Philippines being ranked 129th on the Global Peace Index.[9] Recent developments, such as the Wirecard scandal,[10] have highlighted the possible role of Filipino agents[11] in facilitating multi-billion-dollar cryptocurrency scams. Loopholes in the Philippines highlight the risk associated with Abra. Analysis of these services is important as similar services, such as BitAprica, are being developed for other developing markets.[12] The most recent red flag for Abra came from the U.S. Securities and Exchange Commission (SEC), which fined the company for irregularities in their securities offering to customers outside the U.S.[13]

This article will identify the potential risk associated with crypto-enabled international remittances and the methods being used to operate in a regulatory grey area. The Filipino diaspora, spanning over 100 countries, expands the risk profile of this activity in the Philippines, based on the complex flow of remittances. Some sources estimate the total value of the

imwaltersy / Shutterstock.com

Filipino remittances market to be significantly higher than central bank figures.[14] Based on statistics available,[15] it is unclear whether crypto remittances are being captured based on current recording methods. The Philippines' National Risk Assessment and the Mutual Evaluation Report (MER) both identify remittances as a preferred channel for money laundering and terrorist financing. Unfortunately, the regulatory structures in the Philippines appear to be unsuited to the mixed-use approach being applied to Tambunting pawnshops, 7-Elevens and Abra. For investigators, Abra may provide a potential data source for identifying money laundering and terrorist financing money flows, but the remitter may lack any obligation to assist with such investigations in the Philippines or other jurisdictions where they operate.

The Philippines' National Risk Assessment and the Mutual Evaluation Report (MER) both identify remittances as a preferred channel for money laundering and terrorist financing

Why are Filipino remittances important?

For context, the Filipino remittance industry places the diaspora in the top 100 global economies by GDP, just behind Cameroon and Bahrain.[16] In the Southeast Asian island nation, Tambunting has become a byword for financial assistance amongst Filipinos for decades.[17] This chain of pawnshops allows people to use their belongings as collateral in order to access cash or in this case cryptocurrency. In a country where remittances from abroad are key to the national economy, Tambunting's services are a vital part of the Filipino society. Official figures from Bangko Sentral ng Pilipinas (BSP) show both cash and personal remittances totalling to $33.5 billion in 2019.[18] In June, the remittance industry even showed signs of recovery with a 7.7% increase compared to the same month in 2019.[19] However, Tambunting tellers only require one form of identification for any Tambunting transaction.[20] Many of these forms of identification do not include a photograph, or can be forged easily. Moreover, the Philippines' MER does discuss a number of cases where remittances have been used to launder funds for organized crime and terrorist activity.[21]

Crypto remittances and regulation

Tambunting provides access to digital assets on both Coins.ph and Abra via Electronic Commerce Payments (ECPAY) Inc. Unfortunately, the regulation of pawnshops in the Philippines is anomalous to the regulation of virtual asset exchanges in the country. In most countries, Abra onboarding can be done using a customer's bank account or credit card. In the Philippines, cash onboarding can be done via Tambunting using Abra Tellers[22] and through 7-Eleven via CLiQQ kiosks.[23] CLiQQ kiosks allow for the onboarding of up to 100,000 Philippine pesos (PHP) per day, which is around $2,000 and 62% of the average annual income in the Mindanao region. These kiosks are used for numerous payment services. ECPay is registered as a money services business (MSB), exclusive of electronic money issuers. While Abra does run know your customer (KYC) checks on accounts looking to use a bank account or credit card, the same requirements do not appear to apply to Filipino accounts that only use cash.[24] The anti-fraud solution that Abra has integrated, Simplex,[25] is designed for credit and debit card transactions. The remittance integration, inBestGo, is a Guatemalan-based service that requires information specific to the Guatemalan market.[26] While both Tambunting and CLiQQ provide similar services to Coins.ph, it differs from Abra because it is registered as a remittance and transfer company (RTC) as a virtual currency exchange under the name Betur, Inc. Furthermore, Abra outsources their custody solution to Bittrex,[27] which raises additional challenges for enforcement agencies. Abra's approach capitalizes on apparent regulatory ambiguity in the Philippines by partnering with some businesses that are regulated by BSP and the local SEC, just not as virtual currency exchange services, and others that are not focused on the Filipino or remittance markets.

Risks associated with the Philippines

The prevalence of terrorist activity and organized crime gangs across the Philippines raises concerns around the informal transfer of money in and out of the country. There is also a high rate of extrajudicial killings of people suspected to be involved in drug dealing. At present, the country has the highest murder rate per capita in the Asian region.[28] The Philippines' MER[29] shows that the infrastructure for investigating money laundering and terrorist financing is not very effective in combating the illicit movement of money. This is surprising considering the relatively high level of education[30] in the country and overall size of the Filipino economy.[31] Unfortunately, the controversial new Anti-Terrorism Act of 2020 does little to address terrorist financing in the Philippines beyond removing some oversight measures, such as the requirement for court orders by the Anti-Money Laundering Council (AMLC).[32] These circumstances combine to make the region an ideal target for

Tambunting Pawnshop Boac Branch | Winwin1684 money launderers and terrorist financiers as the infrastructure for such activities is present, i.e., an educated workforce, a weak regulatory structure, an international network of diaspora, and a large economy with the ability to disguise financial flows.

Virtual currency in the Philippines

Based on the AMLC report on the virtual asset transaction profile of exchanges,[33] cryptocurrency had become a significant industry in the Philippines by early 2018. According to the figures from March 6, 2017, to April 10, 2018, from two accredited exchanges, there were over 22,000 suspicious transaction reports (STRs) logged, amounting to over 3.1 billion PHP (approximately $62 million). It is notable that there are now 16 regulated RTCs that provide access to virtual assets.[34] While Abra's Filipino arm is regulated by the Philippines SEC as Plutus Technologies Philippines Corporation, DBA Abra International, they are not registered with the BSP, which regulates the crypto industry across the country. Tambunting Pawnshops are regulated specifically as a pawnshop according to BSP records.[35] As a U.S.-based company, Plutus Financial Inc. is registered as an MSB with the Financial Crimes Enforcement Network to do business across all U.S. states and territories.[36]

Is crypto really being used by criminals in the Philippines and Southeast Asia?

The Philippine Institute for Peace, Violence and Terrorism Research has found evidence that the Islamic State (IS)-linked terror groups in the Philippines are using cryptocurrency to launder funds to support terror networks in the Mindanao region.[37] The report also highlights the reported use of private remittances to fund the siege in Marawi. There are also allegations that another pro-IS group in Indonesia considered using bitcoin for fundraising but eventually dropped the scheme for being too complicated.[38] While many terror groups across Southeast Asia use trusted networks of cash smugglers,[39] there is no reason to believe that these groups would not be prepared to use a more efficient channel to funnel funds in and out of the Philippines. Abra's easy-to-use application is reduce a perceived barrier to entry.

The Philippines have been targeted as a filter hub for scam companies like Wirecard (registered as an electronic money issuer with BSP) looking to avoid attention. Filipino law enforcement agencies have demonstrated the ability to address fraud through STRs. Unfortunately, these agencies currently lack the infrastructure to investigate complex transnational cryptocurrency schemes. This is especially difficult since more than half the population is engaged with the traditional financial system.

Summary

Abra provides an easy method for onboarding clients to cryptocurrency. This reduces the barrier to entry for financial criminals to use cryptocurrency to move and disguise their money as cash remittances. Based on the level of remittances already flowing through the economy, the Tambunting and 7-Eleven off-ramps are susceptible to abuse by bad actors. Unfortunately, Abra has raised red flags around their standards of compliance by having partners that are either not registering in the Philippines, or by having Filipino partners that are not registering to handle e-money as an electronic money issuer or virtual currency as an RTC. Operating in a grey area, as well as avoiding direct regulation and oversight, increases the risk of money laundering and terrorist financing across the Philippines and other jurisdictions where the app operates. The recent SEC decision against Plutus Financial Inc. should draw the attention of investors and enforcement agencies to the company's other activities. Abra's approach to providing minimal oversight for their clients may be favorable in the crypto ecosystem, but the negative impact it can have on "at-risk" countries should not be dismissed in the pursuit of personal profit or marginal improvements to financial services efficiency. While the necessity for anti-money laundering and counter-terrorist financing regulation and compliance in the U.S. can be debated, the purpose of these regulations is to control the flow of funds to bad actors in countries like the Philippines. Abra can choose to comply and assist law enforcement or avoid and assist criminals.

Paul Marrinan, MSc Forensic Computing and Cybercrime Investigation, founder and managing director, Túath Consulting LLC, NY, USA, Paul@marrinan.com

[1] Drew Desilver, “Remittances from abroad are major economic assets for some developing counties,” *Pew Research Center*, January 29, 2018, https://www.pewresearch.org/fact-tank/2018/01/29/remittances-from-abroad-are-major-economic-assets-for-some-developing-countries/.

[2] “Global Financial Inclusion,” *World Bank*, https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=PH

[3] “World bank statistics show that only 34.5% of Filipinos 15+ hold an account,” *World Bank*, https://databank.worldbank.org/reports.aspx?source=1228. World Bank statistics show that only 34.5% of Filipinos 15-years-old and up hold an account.

[4] A decentralized digital payment system that enables peer-to-peer transactions in a secure manner by using a distributed ledger containing all users’ transactions. While the mechanisms used by each digital asset will vary, they are usually based on blockchain technology.

[5] “Tambunting,” *Tambunting*, https://tambunting.ph/Main?profile

[6] “Homepage,” *Abra*, https://www.abra.com/

[7] “What Cryptocurrencies does Abra support?”*Abra*, June 26, 2020, https://support.abra.com/hc/en-us/articles/360001777311-What-Cryptocurrencies-does-Abra-support-

[8] Karen Lema and Manuel Mogato, “Philippines’ Duterte threatens to quit U.N. after drugs war censure,” *Reuters*, August 20, 2016, https://www.reuters.com/article/us-philippines-duterte-un-idUSKCN10W05W

[9] “Global Peace Index 2020,” *Vision of Humanity*, http://visionofhumanity.org/indexes/global-peace-index/

[10] Dan McCrum and Stefania Palma, “Wirecard’s problem partners,” *Financial Times*, March 28, 2019, https://www.ft.com/content/cd12395e-4fb7-11e9-b401-8d9ef1626294. Reports have shown how Filipino shell companies were being used by Wirecard.

[11] Shona Gosh, “The Philippines is investigating Wirecard and its missing $2 billion, and a local lawyer says he’s being framed,” *Business Insider*, June 27, 2020,https://www.businessinsider.com/philippines-wirecard-2-billion-lawyer-framed-2020-6

[12] “BitAprica,” *BitAprica*, https://bitaprica.com/

[13] “SEC have fined Abra previously for breaches of securities law,” *U.S. Securites and Exchange Commission*, July 13, 2020, https://sec.gov/news/press-release/2020-153

[14] “Anti-money laundering and counter-terrorist financing measures: Philippines Mutual Evalution Report,” *Asia-Pacific Group*, October 2019, http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/APG-Mutual-Evaluation-Report-Philippines.pdf, 37.

[15] “Total Number of OFWs Estimated at 2.2 Million,” *Philippine Statistics Authority*, https://psa.gov.ph/statistics/survey/labor-and-employment/survey-overseas-filipinos/table

[16] “GDP by country statistics,” *Worldometer*, https://www.worldometers.info/gdp/gdp-by-country/

[17] Serena Estrella, “Tambunting Pawnshop is the First of Its Kind,” *Remit to the Philippines*, February 7, 2017, https://remit.com.au/tambunting-pawnshop-the-first-of-its-kind/

[18] “Overseas Filipinos’ Remittances,” *Bangko Sentral ng Pilipinas*, http://www.bsp.gov.ph/statistics/keystat/ofw.htm

[19] “June remittances up 7.7% amid recession,” *BusinessMirror*, August 18, 2020, https://businessmirror.com.ph/2020/08/18/june-remittances-up-7-7-amid-recession/

[20] “Valid IDs,” *Tambunting*, https://www.tambunting.ph/Main?ID

[21] “Anti-money laundering and counter-terrorist financing measures: Philippines Mutual Evalution Report,” *Asia-Pacific Group*, October 2019, http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/APG-Mutual-Evaluation-Report-Philippines.pdf

[22] “Where can I find Abra Tellers? Philippines,” *Abra*, https://support.abra.com/hc/en-us/articles/115003984788-Where-can-I-find-Abra-Tellers-Philippines

[23] “How do I deposit into my wallet using EC Pay (CLiQQ kiosk:)? Philippines,” *Abra*, https://support.abra.com/hc/en-us/articles/360034493251-How-do-I-deposit-into-my-wallet-using-EC-Pay-CLiQQ-kiosk-Philippines

[24] “Abra’s Verification Process,” *Abra*, https://support.abra.com/hc/en-us/articles/360018568971-Abra-s-Verification-Process

[25] “Simplex,” *Simplex*, https://www.simplex.com/

[26] “InBestGo,” *InBestGo*, https://inbestgo.com/forms/registros/

[27] “Native Coin Migration,” *Abra*, https://support.abra.com/hc/en-us/articles/360040834752-Native-Coin-Migration

[28] “Murder Rate By Country 2020,” *World Population Review*, https://worldpopulationreview.com/countries/murder-rate-by-country/. The Philippines homicide rate per 100,000 was 11.02% in 2017 according to the United Nations Global study on homicide.

[29] “Anti-money laundering and counter-terrorist financing measures: Philippines Mutual Evalution Report,” *Asia-Pacific Group*, October 2019, http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/APG-Mutual-Evaluation-Report-Philippines.pdf

[30] “Philippines,” *UNESCO UIS*, http://uis.unesco.org/en/country/ph. The Philippines has the highest literacy rate in the Southeast Asia region at 98.2%.

[31] “Philippines GDP,” *Trading Economies*, https://tradingeconomics.com/philippines/gdp. The Philippines GDP was estimated to be $376.8 billion in 2019.

[32] “An Act to Prevent, Prohibit and Penalize Terrorism, Thereby Repealing Republic Act No. 9372, Otherwise Known as the “Human Security Act of 2007,” *The Corpus Juris*, July 3, 2020, https://thecorpusjuris.com/legislative/republic-acts/ra-no-11479.php

[33] “A Study of the Transaction Profile of Accredited Virtual Currency Exchanges in the Philippines,” *Anti-Money Laundering Council of the Philippines*, April 12, 2018, http://www.amlc.gov.ph/images/PDFs/Study%20on%20VC.pdf

[34] “List of Remittance and Transfer Companies (RTC) with Virtual Currency (VC) Exchange Services,” *Bangko Sentral ng Pilipinas*, June 30, 2020, http://www.bsp.gov.ph/banking/MSB.pdf

[35] “List of BSP - Supervised Pawnshops (PSs)” *Bangko Sentral ng Pilipinas*, June 30, 2020, http://www.bsp.gov.ph/banking/pawndir.pdf. BSP has a wide variety of financial services providers recorded under their remit. However, the regulations applicable to pawnshops do not appear to be the same as MSBs and RTCs.

[36] “MSB Registrant Search,” *Financial Crimes Enforcement Network*, https://www.fincen.gov/fcn/financial_institutions/msb/msbstateselector.html#

[37] Amparo Pamela Fabe, “Terrorism Financing Continues Unabated During the COVID-19 Pandemic,” *Philippine Institute for Peace, Violence and Terrorism Research*, May 20, 2020, https://pipvtr.org/2020/05/20/terrorism-financing-continues-unabated-during-the-covid-19-pandemic/. Reports indicate greater use of cryptocurrency to fund terrorist activity in Mindanao.

[38] V. Arianti and Kenneth Yeo Yaoren, “How Terrorists Use Cryptocurrency in Southeast Asia,” *The Diplomat*, June 30, 2020, https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia/

[39] “Regional Risk Assessment on Terrorism Financing 2016: South-East Asia & Australia,” *Australian Transaction Reports and Analysis Centre*, 2016. https://www.austrac.gov.au/sites/default/files/2019-07/regional-risk-assessment-SMALL_0.pdf

BREAKING DOWN BARRIERS TO COMBAT THE ILLEGAL WILDLIFE TRADE

The recently released Financial Action Task Force (FATF) paper entitled, "Money Laundering and the Illegal Wildlife Trade"[1] is a call to action for the private and public sectors. The paper reveals that wildlife trafficking[2] and environmental crime[3] bring in massive profits and are frequently linked to other forms of organized crime including fraud, corruption and money laundering. Thus, it is time to recognize that illegal exploitation of the world's wildlife and environmental crime are global threats.

Illegal wildlife trade (IWT) has significant costs on the environment, biodiversity and public health. In particular, the recent high-profile spread of zoonotic diseases[4] underlines the importance of ensuring wildlife is traded in a legal, safe and regulated manner and that countries remove the profitability of illegal markets.

Transnational organized criminal networks utilize smuggling and money laundering techniques to traffic drugs, people, weapons and other forms of contraband. When these organized criminal networks also exploit poached or illegally harvested wildlife, that means the illicit funds trail also leads back to the financial industry.[5] IWT is perceived by many criminal syndicates as a low-risk, high-profit model. Therefore, anti-money laundering (AML) methods can target these proceeds, identify suspicious transactions in the regulated sector and prevent the smuggling of bulk cash across borders.[6] The purpose of this article is to highlight the important role of public-private partnership in tackling IWT in Hong Kong.

Understanding the nature of the threat

Research published in 2019 indicates Hong Kong's IWT is increasing in volume, is underestimated in value and is contributing to the worldwide extinction crisis.[7] This reflects global trends as the demand for illegal wildlife products increases in the main demand centers of China and other countries in Asia, such as Thailand and Vietnam. The Chinese government has taken active measures to curb this demand; however, environmental crimes, including IWT, are reported to be rising 5% to 7% annually, which is 2-3 times the growth rate of the global economy.[8]

Between 2013 and 2019, customs officers in Hong Kong seized over HK$723 million ($93 million) in trafficked wildlife. These confiscations included over 22 metric tons of ivory, 51 metric tons of pangolins (scales and carcasses), 1,380 metric tons of illegal wood and 27 metric tons of other endangered species (mainly reptiles). Those quantities are conservatively estimated to equate to the deaths of over 3,000 elephants, 67 rhinos and 70,000 pangolins. Depending on which pangolin species, as they vary significantly in maximum size, between 345 and 2,777 pangolins must be killed to produce one ton of scales.

Unsurprisingly, Hong Kong has become recognized as an international hub for IWT, an unfortunate accolade for Asia's World City.[9]

Yet, despite the devastation caused, wildlife and forest crime continue to be viewed as outside mainstream crime by many in the law enforcement community, governments and the public. Cutting-edge investigative techniques often employed in tackling other criminal investigations, such as fraud, human trafficking and drug trafficking, are underutilized for IWT. Using financial and money laundering investigative techniques can substantially enhance wildlife and forest crime investigations.

Unsurprisingly, Hong Kong has become recognized as an international hub for IWT

Following up on the FATF report

FATF guidance recommends more significant high-level political commitment; enhanced operational coordination between law enforcement and the AML industry; better risk awareness and mitigation; enhanced cooperation; and improved private-public collaboration.[10] AML and counter-terrorist financing professionals will immediately find their activity-based approach relevant for this fight. Nongovernmental organizations and professional bodies in Hong Kong are campaigning to include wildlife crime offenses under Schedule 1 of Cap. 455 (Organized and Serious Crimes Ordinance) to further deter transnational criminal enterprises who use Hong Kong as a major port and transport hub for wildlife smuggling. Without access to the coercive investigative powers available under the Organized and Serious Crimes Ordinance section, the Hong Kong Customs and Excise Department is unlikely to gather sufficient evidence to pursue charges effectively against offenders for dealing with the proceeds of wildlife crimes.

Confiscated ivory, at HQ of Dzanga-Sangha Special Reserve, Central African Republic. © Andy Isaacson / WWF-US.

Steve Oberholtzer, special agent for the U.S. Fish and Wildlife Service, holds an ivory tusk at the Rocky Mountain Arsenal National Wildlife Refuge Repository in Commerce City, Colorado. © Jamie Cotten / IFAW / WWF-US.

Converging approaches (private sector and law enforcement)

In 2019, FATF, under President Xiangmin Liu of China, made it a priority to help countries go after the money involved in IWT as well as identify and disrupt large criminal networks that profit from this crime. On November 22, 2019, FATF President Liu hosted one of the first regional meetings on tackling IWT as a financial crime in Beijing. It was the first time that public and private sector representatives, including AML experts and wildlife experts, came together to share experiences about detecting and combating the financial flows linked to the IWT.

The FATF German presidency (2020-2022) aims to expand on the work to prevent IWT by focusing on the broader issue of environmental crime and its connections with money laundering and terrorist financing. The work will analyze financial flows linked to environmental crime to raise awareness of pertinent money laundering and terrorist financing risks as well as to inform possible further work on potential policy implications.

The importance of public-private partnership

As a global financial center, Hong Kong strives to meet international standards for gathering intelligence to detect illicit cross-border fund flows and interdict them. The Hong Kong special administrative region government created the Fraud and Money Laundering Intelligence Taskforce (FMLIT), which is composed of the Commercial Crime Bureau of the Hong Kong Police Force, in collaboration with the Hong Kong Monetary Authority, the Hong Kong Association of Banks and a number of banks. The FMLIT facilitates public-private partnership to enhance the detection, prevention and disruption of serious financial crimes and money laundering activities through effective information and intelligence sharing.

The financial sector plays a crucial role in investigating and identifying suspicious activity. Dialogue between the public and private sector is vital for assisting financial institutions (FIs) and law enforcement agencies in identifying suspicious activity and in maintaining an up-to-date understanding of IWT threats and risks. A critical step is creating public-private partnerships and improving international cooperation to identify and disrupt the illicit proceeds of this devastating criminal activity.

On June 13, 2019, the U.S. Attorney's Office in the Southern District of New York indicted four individuals charged with participating in a conspiracy to traffic more than $7 million in rhino horns and elephant ivory. In addition, suspects were charged with conspiracy to commit money laundering, and with participating in a conspiracy to distribute and possess with intent to distribute more than 10 kilograms of heroin.[11] The case was a model of public-private collaboration across agencies and continents on wildlife trafficking with links to transnational organized crime and money laundering.

4P model—A whole system response to tackling IWT

Over the last few years, criminal networks have continually adopted sophisticated and agile business models to ensure that they continue to proliferate. It became clear that an innovative approach was needed and that one organization alone could not tackle the threat as it has impacted all sectors and communities. A whole system response was required to have maximum impact on disrupting criminal networks. In the United Kingdom (U.K.), law enforcement agencies endorsed and implemented the following 4P approach for tackling serious and organized crime, including drug trafficking, human trafficking, and child sexual abuse and exploitation online:

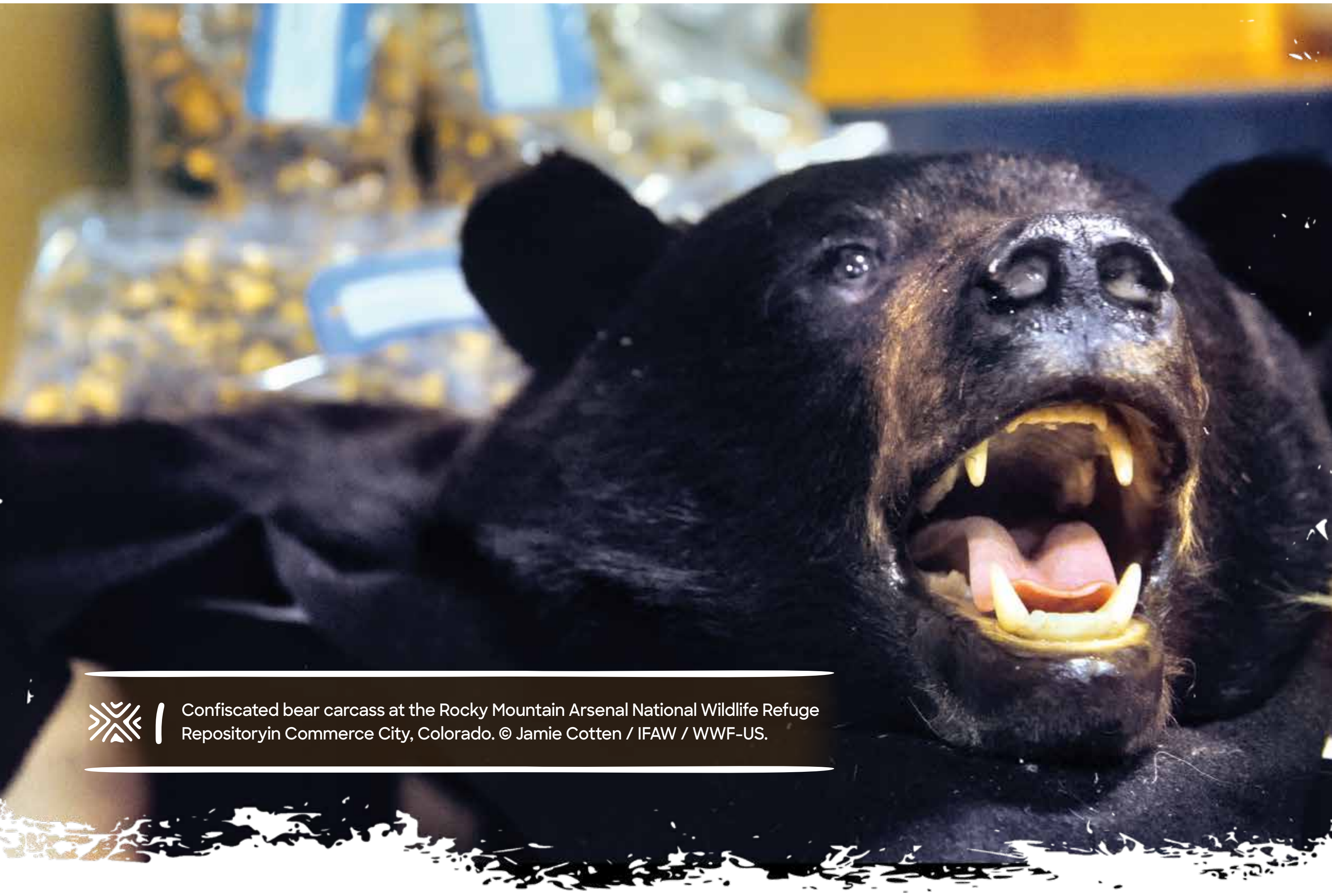
- **Pursue:** Enhance the intelligence and operational response and pursue criminal networks through prosecution and disruption.
- **Prevent:** Identify risk factors in terms of criminality, ability, networks and identity; focus on preventing criminal networks from engaging in criminal activity; and have an effective response through collaboration on prevention strategies with regional and international partners, tackling the threat upstream and at the source.
- **Protect/prepare:** Increase protection against serious and organized crime and reduce the impact of this criminality where it takes place.

Given the domestic, regional and global reach of IWT, a similar approach was needed to tackle it. The UK's Serious and Organised Crime Network (SOCnet) Illicit Finance lead with invaluable support from World Wide Fund for Nature, ACAMS and other key stakeholders, produced a high-level 4P model for tackling IWT in Hong Kong that highlighted collaboration across all sectors on key initiatives to combat IWT—a whole system response (see Table 1).

Table 1:

4P framework

PURSUE	PREVENT	PROTECT/PREPARE
Improved capacity of financial institutions in identifying/reporting financial transactions linked to IWT	**Increased capability in tackling IWT in key sectors through the use of technology, innovative tools and techniques**	**Increased awareness and delivery of resource materials/training to build resilience in communities and sectors**
· Financial crime intelligence roundtables: A key public-private partnership platform to drive progress · Progress institutionalizing IWT red flags and risk assessment indicators in credit risk assessment and valuation for loans · Maritime/shipping roundtables on IWT focused on identifying and agreeing on a plan of action for key gaps, red flags and risk indicators · Campaigning on the inclusion of IWT within Section 1 of the Organized and Serious Crimes Ordinance	· Develop a successful industry collaboration forum for sharing best practices, typologies and reports · Collective action by ACAMS members on counter-IWT financial crime investigation · Brief heads of shipping companies on IWT including routes, use of technology and red flags · Deliver compendium toolkit for shipping sector including red flags, typologies and risk indicators · Develop IWT money flows project toolkit based on risk indicators and red flags for the financial sector	· Raise awareness through key platforms and delivery of targeted communication campaigns—whole system response · Briefings to cross-sector influential committees and boards highlighting key risk indicators and impact to secure commitment on future initiatives · Develop training/comprehensive guide to build IWT alerts/red flags for the financial and private sector · Develop course for port operators on addressing maritime-related IWT · Delivery of tailored IWT chapters in Asia-Pacific, Europe, Latin America and Australasia



Confiscated bear carcass at the Rocky Mountain Arsenal National Wildlife Refuge Repositoryin Commerce City, Colorado. © Jamie Cotten / IFAW / WWF-US.

The HK framework

Building on a pilot project led by Standard Chartered Bank with WWF, the Hong Kong framework creates roundtable forums and working groups composed of banking AML professionals, regulatory and law enforcement representatives, and nonprofit organizations. The objective is to bring together technical expertise to address the challenges. In addition, the initiative targets explicitly raising awareness across knowledge domains and socializing concerns. An imperative is building an educational program along with tools to be leveraged by collaborators.

The table below outlines three immediate outcomes. Outcome 1 targets information sharing to improve detection and reporting by harnessing ACAMS chapters and events. In contrast, Outcome 2 develops cross-industry working groups to enhance red flags, alert scenarios and risk assessment indicators that can be ingested into systems. Outcome 3 shapes an intelligence-led and information-sharing approach.

> The Hong Kong framework creates roundtable forums and working groups composed of banking AML professionals, regulatory and law enforcement representatives, and nonprofit organizations

Table 2:

Immediate outcomes

Outcome 1	Output 1.1	Activity 1.1
Financial intelligence units and banking industry financial compliance investigators take part in advanced identification, reporting and mitigation of wildlife trafficking-related money laundering	Improve the capacity of financial institution staff and AML compliance officers in identifying and reporting financial transactions linked to wildlife trafficking	1.1.1 Virtual financial crime intelligence roundtables on IWT for Thailand, Malaysia, Hong Kong and potentially Singapore 1.1.2 Develop training materials (video and online training production, i.e., motion graphics on IWT financial crime and corruption)
Outcome 2	**Output 2.1**	**Activity 2.1**
Improve the financial red flags and key risk indicators for financial institution enterprise systems	Enhance existing financial flows red flags and key risk indicators and support institutionalizing IWT red flags and risk assessment indicators	2.1.1 Develop red flags and key risk indicators through private-public workshops 2.1.2 Support the institutionalizing IWT red flags and risk assessment indicators into risk assessment and valuation for loans
Outcome 3	**Output 3.1**	**Activity 3.1**
Collaboration in financial sector enforcement occurs as intended through improved stakeholder cooperation, enhanced capacity of both private and government stakeholders, and implementing plans and policies to counter IWT	Facilitate ACAMS-led collective action in coordination on IWT with law enforcement networking	3.1.1 One significant collective action by ACAMS members on counter-IWT financial crime investigation mentoring to participants/ ex-trainees (three months) 3.2 Final report and analysis of collective action by ACAMS

One of 16 tiger cubs seized from smugglers. A veterinary team from the wildlife forensic unit take blood samples to trace the DNA. Chaiyaphum, Thailand. © WWF / James Morgan.

Closing the circle

If communities have a unified and targeted approach, then there can be measurable impact on the IWT value and supply chain including improved detection, which would result in increased scrutiny and pressure on suspected brokers, exporters/importers, wholesalers and retailers who exploit the vulnerabilities in the system. We are happy to announce this 4P framework in Hong Kong and encourage ACAMS chapters to adopt a similar approach.

Compliance officers are uniquely competent in that they can contribute intelligence on illicit money flows and they can examine trade flows resulting in the destruction of protected species, fauna and flora. If COVID-19 has shown anything to the world, it is that everyone must unite to protect what has long been considered the heart of the planet–the environment and the wildlife within it—so future generations have an equal chance to cherish it as well.

Brian V. Gonzales, head of protection of endangered species, WWF, Hong Kong SAR, China, bgonzales@wwf.org.hk

Chinali Patel, consul, international illicit finance policy lead, British Consulate-General, Hong Kong SAR, China

Dr. William Scott Grob, CAMS-FCI, AML director-APAC, Hong Kong SAR, China, wsgrob@acams.org

[1] “Money Laundering and the Illegal Wildlife Trade,” *Financial Action Task Force*, June 2020, https://www.fatf-gafi.org/media/fatf/documents/Money-laundering-and-illegal-wildlife-trade.pdf

[2] “The Pangolin Reports: Trafficked to Extinction,” *ADM Capital Foundation*, September 25, 2019, https://www.admcf.org/research-reports/the-pangolin-reports-trafficked-to-extinction/

[3] “Stopping Illegal Logging,” *World Wide Fund for Nature*, https://www.worldwildlife.org/initiatives/stopping-illegal-logging

[4] Zoonotic diseases are derived from viruses, bacteria and other pathogens that are transmitted between animals and humans. According to the World Health Organization, some 60% of emerging infectious diseases that are reported globally are zoonotic (including SARS, Ebola, COVID-19 and MERs).

[5] “Enhancing the Detection, Investigation, and Disruption of Illicit Financial Flows from Wildlife Crime,” *Asia/Pacific Group on Money Laundering and the United Nations Office on Drugs and Crime*, 2017, https://globalinitiative.net/wp-content/uploads/2018/01/APG-UNODC-Wildlife-Crime-Report.pdf

[6] “Financial flows from wildlife crime,” *United Nations Office on Drugs and Crime*, https://www.unodc.org/documents/Wildlife/Financial_Flow_Wildlife_Crime.pdf

[7] Sam Inglis, “Trading in Extinction: The Dark Side of Hong Kong’s Wildlife Trade,” *ADM Capital Foundation*, January 21, 2019, https://www.admcf.org/2019/01/21/shedding-light-illegal-trade-hong-kong-high-volume-lucrative-black-market-business/

[8] Christian Nellemann et. al, “The Rise of Environmental Crime – A Growing Threat To Natural Resources Peace, Development And Security,” *The United Nations Environment Programme and Interpol*, https://reliefweb.int/sites/reliefweb.int/files/resources/environmental_crimes.pdf

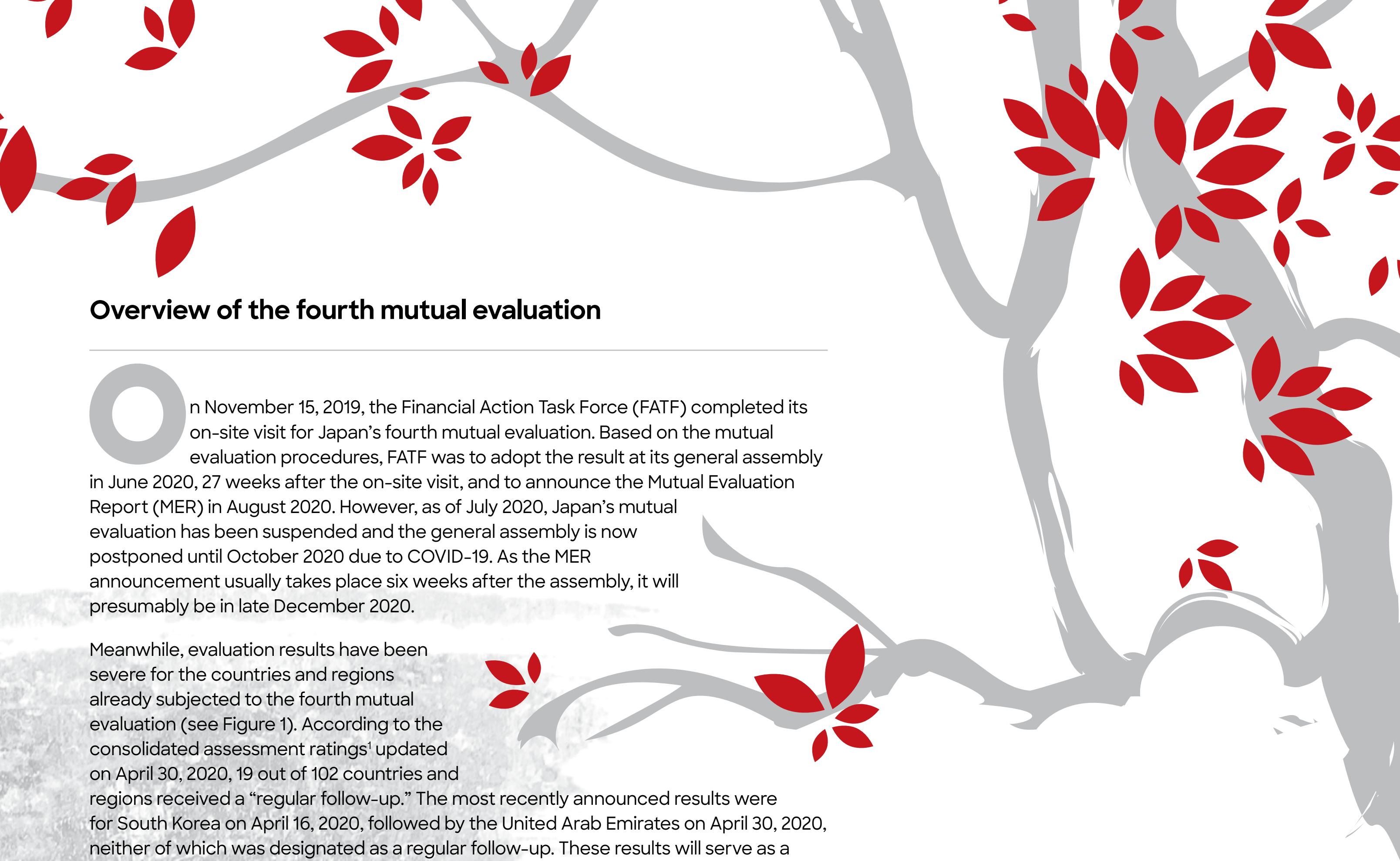
[9] Daan P. van Uhm, *The Illegal Wildlife Trade: Inside the World of Poachers, Smugglers and Traders*, (Springer International Publishing, 2016).

[10] “Money Laundering and the Illegal Wildlife Trade,” *Financial Action Task Force*, June 2020, https://www.fatf-gafi.org/media/fatf/documents/Money-laundering-and-illegal-wildlife-trade.pdf, 57-59.

[11] John Cusack, “Wildlife Trafficking Syndicate ensnared by United Forces,” *Financial Crime News*, June 2019, https://thefinancialcrimenews.com/wildlife-trafficking-syndicate-ensnared-by-united-forces/

Japan's AML/CTF efforts in the present and beyond

第4次対日相互審査の結果公表に備えたマネー・ローンダリングおよびテロ資金供与対策（AML/CFT）の高度化



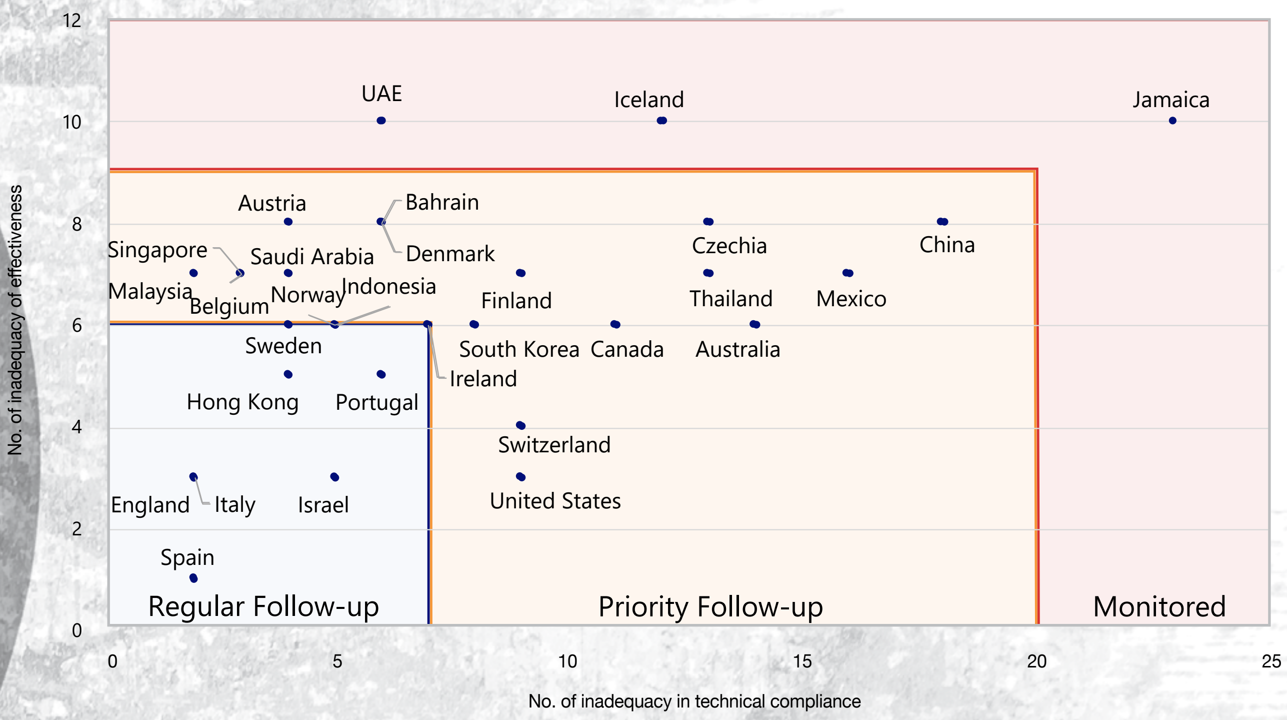
Overview of the fourth mutual evaluation

On November 15, 2019, the Financial Action Task Force (FATF) completed its on-site visit for Japan's fourth mutual evaluation. Based on the mutual evaluation procedures, FATF was to adopt the result at its general assembly in June 2020, 27 weeks after the on-site visit, and to announce the Mutual Evaluation Report (MER) in August 2020. However, as of July 2020, Japan's mutual evaluation has been suspended and the general assembly is now postponed until October 2020 due to COVID-19. As the MER announcement usually takes place six weeks after the assembly, it will presumably be in late December 2020.

Meanwhile, evaluation results have been severe for the countries and regions already subjected to the fourth mutual evaluation (see Figure 1). According to the consolidated assessment ratings[1] updated on April 30, 2020, 19 out of 102 countries and regions received a "regular follow-up." The most recently announced results were for South Korea on April 16, 2020, followed by the United Arab Emirates on April 30, 2020, neither of which was designated as a regular follow-up. These results will serve as a touchstone for Japan.

Figure 1:

The status of FATF's mutual evaluation



Source：Created by NRI, from FATF Consolidated assessment ratings (Updated 30 April 2020)
Horizontal axis is number count of PC and NC, and horizontal axis is number count of ME, certain countries and regions are plotted and LE
In addition to mutual evaluation, the latest results were adopted for countries where follow-up reports were published

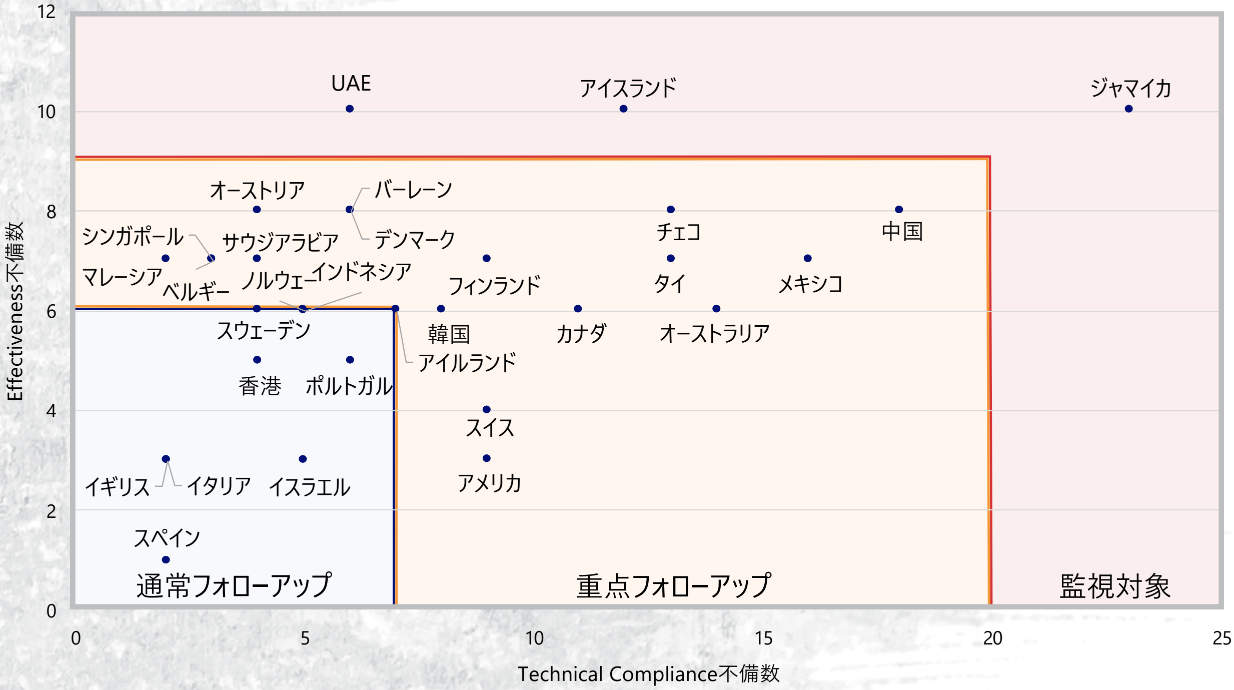
1. FATF第4次相互審査の概況

2019/11/15にFATF第4次対日相互審査のオンサイトレビューが完了した。当初はFATF相互審査手続きに則り、オンサイトレビューから数えて27週に相当する2020年6月開催のFATF総会にて審査結果が審議・採択、次いで2020年8月に審査結果報告書（MER: Mutual Evaluation Report）が公表される予定であった。しかし2020年7月現在、COVID-19の影響により対日相互審査手続きは凍結状態にあり、FATFからは対日相互審査結果の審議・採択を2020年10月開催の総会へ順延する旨が発表されている。MERの公表は総会から数えて6週前後であるため、2020年12月後半になると想定される。

また既にFATF第4次相互審査を受けた国・地域に対しては、概して厳しい評価が続いている。2020年4月30日付更新の統合審査結果[1] によると、これまで審査を受けた102の国・地域のうち通常フォローアップと判定されたのは19の国・地域である。直近では2020年4月16日に韓国、2020年4月30日にUAEの審査結果が発表されたが、いずれも通常フォローアップ入りはならなかった。

Figure 1:

FATF第4次相互審査の状況



出典：FATF Consolidated assessment ratings (Updated 30 April 2020) よりNRI作成
横軸はPCおよびNC、縦軸はMEおよびLEを計数し、一部国・地域をプロット
相互審査に加えてフォローアップレポートが公表された国・地域は最新結果を採用

Current conditions of AML/CTF in Japan

According to the United Nations Office on Drugs and Crime (UNODC),[2] the estimated amount of money laundering worldwide is between 2% to 5% of Gross Domestic Product (GDP) or between $800 billion and $2 trillion per annum. Since statistics detailing the estimated amount of money laundering have not been made public, if one simply multiplies with a ratio to Japan's nominal GDP, the domestic amount would be astounding—5 to 13 trillion yen ($47 billion to $123 billion) annually. However, Japan's National Police Agency calculates the damage from special fraud is 31.58 billion yen ($300 million) and "The White Paper on Police 2019"[3] reported 511 arrests related to money laundering.

There have been no cases of money laundering where fines were imposed and no large-scale terrorism has occurred since the Tokyo Sarin attack a quarter century ago. Therefore, money laundering and terrorism were never seen as commonplace. According to the 2019 "Annual Report Regarding Act on Prevention of Transfer of Criminal Proceeds,"[4] there were 1,123 arrests due to suspicious transactions, of which 933 suspicious transaction report (STR)-initiated cases and 493 STR use cases of fraud-related crimes accounted for the majority.

The following legislation has been enacted (in addition to the pre-existing Foreign Exchange Act and Anti-Drug Special Provisions Law) based on the FATF 40 and the IX Recommendations:

- Act on Prevention of Transfer of Criminal Proceeds (2008/3)
- Amended Act on Prevention of Transfer of Criminal Proceeds (2013/3)
- Amended Act on Punishment of Terrorist Financing (2014/12)
- International Terrorist Asset-Freezing Act (2015/10)
- Amended Act on Prevention of Transfer of Criminal Proceeds (2016/10)
- Amended Act on Prevention of Transfer of Criminal Proceeds (2017/4)
- Amended Act on Punishment of Organized Crimes (2017/7)

An update to the new FATF 40 Recommendations, publication and revision of the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (AML/CTF guidelines), as well as a revision of "Reference Cases on Suspicious Transactions" have all been implemented:

- Announcement of AML/CTF guidelines (2018/2)
- Revision of AML/CTF guidelines (2019/4)
- Revision of Reference Cases on Suspicious Transactions (2019/4)

However, the AML/CTF guidelines are regarded as supervisory viewpoints of the Financial Services Authority (FSA), and the legal ground for enforcing administrative measures are business laws, such as the Banking Act and the Financial Instruments and Exchange Act.

2. 日本におけるAML/CFTの現状

UNDOC[2] によると、全世界のマネー・ローンダリング推計額は全世界GDPの2%～5%、額にしてUS$8,000億～US$2兆/年である。国内のマネー・ローンダリング推計額に関連した統計情報は公開されていないため、単純に全世界における日本の名目GDP比率5.9%（2018年）に掛け合わせると国内推計額は約5兆円～13兆円/年と巨額になる。警察庁からは「特殊詐欺認知・検挙状況等[3] 」が公表されているが、特殊詐欺の被害額は315.8億円（2019年確定値）であり、上記推計値からは大きな開きがある。また「警察白書[4] 」（2019年版）によるとマネー・ローンダリング関連事犯の検挙件数は511件である。

加えて国内においては制裁金が課徴されたマネー・ローンダリングは発生しておらず、大規模なテロは1995年の地下鉄サリン事件以来25年間発生していない。このためマネー・ローンダリングやテロは身近な存在と言い難く、「犯罪収益移転防止法に関する年次報告書[5] 」（2019年）によると、疑わしい取引に関する情報を端緒として検挙した1,123件のうち詐欺関連事犯が933件、活用事件数は493件中と最多を占めている。

一方、法制面では旧来から存在する外為法や麻薬特例法に加えて主に下記の関連法が施行されたが、FATF第3次対日相互審査、すなわち「旧40の勧告＋9の特別勧告」を源流とするものであり、リスクベース・アプローチ（RBA）の強化や国内外PEPs、税犯罪、大量破壊兵器等の新たな脅威への対応を中心とした「新40の勧告」に対しては不足感が否めない。

- 犯罪収益移転防止法全面施行（2008/3）
- 改正犯罪収益移転防止法全面施行（2013/3）
- 改正テロ資金提供処罰法施行（2014/12）
- 国際テロリスト財産凍結法施行（2015/10）
- 改正犯罪収益移転防止法全面施行（2016/10）
- 改正犯罪収益移転防止法全面施行（2017/4）
- 改正組織的犯罪処罰法施行（2017/7）

「新40の勧告」への補強としては下記の通り「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」（AML/CFTガイドライン）の公表および改訂、「疑わしい取引の参考事例」の改訂が実施されている。しかしAML/CFTガイドラインは金融庁による監督項目の位置付けであり、行政処分を実施するための法的な裏付けは銀行法や金融商品取引法等の各業法規制である。

- AML/CFTガイドライン公表（2018/2）
- AML/CFTガイドライン改訂（2019/4）
- 疑わしい取引の参考事例改訂（2019/4）

Five potential points of Japan's MER

In light of the MERs and their follow-up reports on other countries and regions, as well as the current status of AML/CTF in Japan, the MER of Japan will presumably raise the following five points:

1. **Compulsory enforcement of AML/CTF guidelines (or something equivalent):** Following FATF's third mutual evaluation of Japan, the FSA's supervisory policy was not regarded as "legally enforceable." Whether or not the AML/CTF guidelines are to be seen as appropriate means accompanying laws and regulations will be quite significant.
2. **Implementation of fines and penalties:** In addition to fines resulting from extraterritorial application of the USA PATRIOT Act, which have exceeded $15 billion since 2013, and in consideration of the fines and penalties against executives in Asian countries, administrative measures alone may be seen as "lesser" compared to other countries. For instance, if one conceals proceeds from crimes, he would be considered as violating the Act on Punishment of Organized Crimes, punishable by up to five years in prison, fines of 3 million yen ($28,000) or less, or both imposed cumulatively. Moreover, the AML/CTF guidelines require senior management to understand AML/CTF risk and to be actively involved, but on-site engagement by senior management has at times been insufficient. Therefore, the laws may become stricter in the future to clarify where the responsibility lies.
3. **Improvement of the quality of registered suspicious transactions:** In light of pointing out the quality of suspicious transactions, improving the use of suspicious transactions may be noted as well. While the Japan Financial Intelligence Center (Japan's financial intelligence unit) has been making its annual reports and "Criminal Proceeds Transfer Risk Level Investigation Report" available, the Financial Crimes Enforcement Network (FinCEN) has a website from which suspicious activity data can be extracted in multiple ways.[5] In addition, FinCEN has made a method for submitting suspicious activity reports in XML format available, which may be useful for data utilization.[6]
4. **Sophistication in continuous know your customer (KYC):** Regarding customer information, financial institutions (FIs) have been rapidly upgrading the onboarding phase, which may require implementing continuous KYC including updating customer information and transaction risk periodically. As seen in overseas cases, a customer who had been dealing in a nonproblematic way a while after onboarding could suddenly start to remit to a company affiliated with North Korea. Stipulated in the AML/CTF guidelines as "required actions for a financial institution," establishing an AML/CTF risk management program with a risk-based approach (RBA) and continuing risk management will be required more than ever.
5. **Improvement of the quality of information (including that of beneficial owners):** Because FATF methodology does not allow confirmation based on self-reported information, it may be pointed out that company registration within Japan is based on self-reporting. As domestic commercial databases are also

３. FATF第４次対日相互審査結果の見通し

これまでの他の国・地域へのMERやフォローアップレポートと日本におけるAML/CFTの現状を照らし合わせると、以下５点が主な指摘として挙がる可能性があると考える。

①　AML/CFTガイドラインの強制化、もしくはそれに準ずる法制化

2008年のFATF第3次対日審査時に金融庁の監督指針が「法的な執行力を有する手段」と認められなかった過去事例を踏まえると、今回のFATF第4次対日相互審査においては、前述の通り各業法規制と合わせてAML/CFTガイドラインが当該手段と認められるかが大きなポイントとなる。

②　制裁金・懲罰の制定

2013年からの制裁金累計額がUS$150億を超過した米国愛国者法の域外適用に加え、アジア各国における制裁金や役職者個人への懲罰が顕著な傾向にあることを踏まえると、行政処分のみでは他国と比較して"軽い"と判断される可能性がある。例えば犯罪収益を隠匿した場合、「組織的な犯罪の処罰及び犯罪収益の規制等に関する法律10条」の適用により5年以下の懲役もしくは300万円以下の罰金または併科である。

またAML/CFTガイドラインでは経営陣がAML/CFTリスクを理解し積極的に関与することを求めているが、コンプライアンスの現場からは経営陣の関与不足を嘆く声も聞かれる。このため、責任の所在を明確化する意味合いからも厳罰化される可能性がある。

③　疑わしい取引の届出の質向上

MERにおける疑わしい取引の届出の質に関する指摘を踏まえると、国内の疑わしい取引の届出の利活用に関する改善が指摘される可能性がある。

日本の資金情報機関(FIU: Financial Intelligence Unit)である犯罪収益移転防止対策室（JAFIC）からは主に前述の「犯罪収益移転防止法に関する年次報告書」および「犯罪収益移転危険度調査書」が提供されているのに対して、例えばアメリカのFIUであるFinCENは複数の切り口からデータを抽出可能なウェブサイト公開している。[6]

またFinCENでは疑わしい行為（SAR: Suspicious Activity Report）をXML形式で提出できる接続方法を公開しており[7]、データ活用にも利する面があると考える。

based on self-reporting, many FIs have difficulties in collecting beneficial ownership information. This awaits legislation in response to the FATF Recommendations.

Improving AML/CTF in anticipation of Japan's mutual evaluation results

The revision or new establishment of AML/CTF guidelines is largely dependent on whether FATF will regard the current guidelines as legally enforceable. At any rate, it is highly probable that the "next shift" will take place on or about the publication of the MER in December 2020. Until then, FIs should prepare for the upcoming AML/CTF advancements by taking the following steps.

First, it is the highest priority to update customer information to the latest available information. Although the level of difficulties could vary depending on the number of accounts and types of transactions, it is presumed that updating customer information will be a minimum request from authorities.

Next, quantify customer risk. In quantification of customer risk, FIs can refer to the preceding cases from global systemically important financial institutions (G-SIBs). Following a risk assessment report submitted to FSA, FIs first construct a simple customer risk model with inherent risk and residual risk. One should not aim for the best risk model from the onset, but it is recommended to start with approximately 10 types of risk factors, periodically adding and removing risk factors, and eventually completing the construction of an effective model.

As for the customer filtering, FIs first deal with politically exposed persons (PEPs) as indicated in the MER. In Japan, due diligence for domestic PEPs is voluntary; however, it is required to adhere to FATF Recommendations 12 and 22, and because it has become a norm to include tax evasion and corruption, early rulemaking is desired.

During transaction monitoring, FIs should translate transaction risk to customer risk. By promptly determining ongoing customer risk, FIs can realize a better risk-based approach. FIs are also able to detect a customer who "changes" some time after opening an account.

In addition, domestic systemically important banks (D-SIBs) and other major FIs will need to put a priority on trade-based money laundering (TBML) and weapons of mass destruction. These cases are difficult to detect with a traditional rule-based scenario with thresholds for the transaction amounts and frequencies, as FIs need to align customer information, transaction data and trade-related data. For instance, there could be a comprehensive judgment that takes shipping documents, market price and anchorage sites into consideration. However, information required is so vast that investigators have limitations to gather and analyze. As such, one promising solution would be using the network analysis solutions that have started to be adopted by some G-SIBs.

On the other hand, for authorities, it would help improve the "Jigyosha Program," an STR submission program, by adding flexible data formats such as XML. This also adds flexibility to the program

④　　継続的顧客管理の高度化

顧客情報に関して各金融機関においては急ピッチで最新化作業、言わばオンボーディング断面の整備が行われているが、オンゴーイングな顧客情報の更新、さらには取引リスクも勘案した継続的顧客管理を求められる可能性がある。

オンボーディング当初は問題ない取引を行っていた顧客が一定期間経過後に突如として北朝鮮関連企業への送金を開始したことを検知出来なかったことにより、金融機関が当局に起訴された海外事例に見られるように、オンゴーイングな顧客管理の必要性も高まっている。

AML/CFTガイドラインで規定された【対応が求められる事項】、とりわけミニマム・スタンダードであるRBAによるAML/CFTリスク管理態勢の構築は当然として、維持に関してはこれまで以上に実現要請が強まることは確実であろう。

⑤　　実質的支配者を含む情報の質向上

FATFメソドロジーでは自己申告情報に基づく確認は不可とされているところ、国内の法人登記が自己申告制である点を指摘される可能性がある。

国内の商用データベースにおいても法人登記情報は自己申告情報に基づいているため、特に実質的支配者情報等の徴求には苦慮している金融機関が多いと推測される。この点においては、むしろFATFからの指摘を契機にした法制化等の改善が望まれる。

4. FATF第４次対日相互審査の結果公表に向けたAML/CFTの高度化

AML/CFTガイドラインの改訂もしくは法規制改訂や新設は、ガイドラインが法的執行力を有するとFATFに認められるかに依るところが大きい。しかし、いずれにしても2020年12月のMER公表前後には"次の動き"がある可能性が高い。それまでの間、各金融機関においてはRBAによるAML/CFTリスク管理体制を構築し、今後のAML/CFT高度化に備えるべきであろう。具体的には以下の通りである。

- 第一に顧客情報最新化の完遂が最優先である。2018年2月のガイドラインの公表から2020年末で約3年が経過する。口座数の多寡や取引形態等により難易度は異なるものの、顧客情報の最新化については当局からの要請も相応になるものと推測する。
- 次いで顧客リスクの定量化である。顧客リスクの定量化においては、先行するG-SIBs等の事例が参考になる。リスク評価書に従い、まずは各金融機関における固有リスクや残存リスクをリスク要素としたシンプルな顧客リスクモデルを構築する。最初からベストなリスクモデルを狙わず、目安として10種類弱のリスク要素を選択したモデルから開始し、定期的にリスク要素の追加・削除を実施することにより徐々に実効性の高いモデルへ仕上げていくことを推奨する。

when authorities modify items for future advancements. Moreover, data formats such as XML have high connectivity with existing AML/CTF systems in FIs, to reduce administrative burdens as well as burdens of systems for FIs.

Conclusion

FIs in Japan should make hay while the MER is on its way. Whatever the MER will be, FIs should reframe their own AML/CTF programs to at least to meet the RBA. Both the risk assessment at onboarding and ongoing reassessments are essential. By gaining a foothold, FIs now can advance themselves and become durable to combat money laundering and terrorist financing.

Atsuo Takada, CAMS, senior systems analyst, Nomura Research Institute, Ltd., a-takada@nri.co.jp

[1] "Consolidated Assessment Ratings," *Financial Action Task Force*, http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html

[2] "Money-Laundering and Globalization,"*United Nations Office on Drugs and Crime*, https://www.unodc.org/unodc/en/money-laundering/globalization.html

[3] "White Paper on Police," *Japan National Police Agency*, 2019, https://www.npa.go.jp/hakusyo/r01/index.html

[4] "Annual report on prevention of transfer of criminal proceeds," *Japan National Police Agency*, 2019, https://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/data/jafic_2019e.pdf

[5] "Suspicious Activity Report Statistics (SAR Stats)," *Financial Crimes Enforcement Network*, https://www.fincen.gov/reports/sar-stats

[6] "Supported Methods of Transmission," *BSA E-Filing System Financial Crimes Enforcement Network*, https://bsaefiling.fincen.treas.gov/MethodsOfTransmission.html

- 顧客フィルタリングはMERで指摘が挙がっているPEPs対応が高優先となろう。日本においては国内PEPsへの対応は任意だが、FATF勧告12および22において対応が求められていること、広義のマネー・ローンダリングに脱税および汚職を含めることが趨勢であることから、早晩の対応が求められるであろう。

- 取引モニタリングにおいては、継続的顧客管理の観点から取引リスクを顧客リスクへ還元する点を実現したい。AML/CFTガイドラインでは【先進的な取組み事例】に相当するが、オンゴーイングの顧客リスクを適時に把握することにより真のRBAが実現され、前述のような口座開設の一定期間後に“化ける”顧客の検知も可能になると考える。

- またD-SIBsおよび主要金融機関においてはTBMLや大量破壊兵器拡散防止への対応も優先事項となろう。これらは旧来の取引金額や頻度によるルールベースシナリオでは検知が困難であり、顧客情報や取引データに加えて貿易関連データ等との連携が必要になる。例えばTBMLであれば船積書類や市況価格、寄港地等を加えた総合的な判断が必要になるが、情報が非常に広範に渡るため人手による情報収集・分析には限界がある。このため、例えば一部G-SIBsで採用が始まっているネットワーク分析ツールが有望な解になるであろう。

一方で、当局においては事業者プログラムの届出様式改修が一助になるであろう。

- 届出様式にXML等の自由度の高いデータ形式を追加することにより、疑わしい取引データの利活用が容易になる上に、今後の徴求項目の増減に柔軟に対応出来る。

- またXML等のデータ形式は、金融機関側の既存AML/CFTシステムとの接続性も高く、AML/CFTにかかる事務およびシステム負担軽減にもつながるであろう。

以上

高田貴生, CAMS, 上級システムアナリスト, 野村総合研究所
a-takada@nri.co.jp

[1] http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html

[2] https://www.unodc.org/unodc/en/money-laundering/globalization.html

[3] https://www.npa.go.jp/publications/statistics/sousa/sagi.html

[4] https://www.npa.go.jp/hakusyo/r01/index.html

[5] https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/data/jafic_2019.pdf

[6] https://www.fincen.gov/reports/sar-stats

[7] https://bsaefiling.fincen.treas.gov/MethodsOfTransmission.html

The travel rule challenge:

Virtual asset transfers versus wire transfers

「暗号資産・暗号資産交換業者に関する新たなFATF基準についての12ヵ月レビュー」におけるトラベルルールの課題 - 暗号資産移転と銀行送金を比較して

It's been several years since financial authorities began to witness the rise of virtual assets and blockchain technologies throughout the world. Regardless of the technology underlying each financial service, the challenge has been how to apply technology-neutral regulation so that similar anti-money laundering/counter-terrorist financing (AML/CTF) risks, such as misuse by illegal customers or inflow of illicit funds, are subject to the same regulation.[1] While taking into account the conveniences provided by virtual assets, authorities are now considering how to administer appropriate regulation and supervision to protect consumers and prevent money laundering, terrorist financing and proliferation financing.

In July 2020, the Financial Action Task Force (FATF) published the "12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers"[2] (the Report). The financial authorities, including the Financial Services Agency of Japan (FSA), have notified the public of this release to catch the attention of many stakeholders, including ACAMS members.

This article will explain the "travel rule" and its application for virtual asset transactions, which is one of the hot topics in the Report, by comparing them with FATF provisions for financial institution (FI) transfers.

Background of the Report

Figure 1 is the revision process of the FATF Standards that triggered virtual asset service provider (VASP) monitoring.

2020年7月、「暗号資産・暗号資産交換業者に関する新たなFATF基準についての12ヵ月レビューの報告書」（以下「本報告書」）をFATFが公表した。本邦金融庁を含む 、様々な金融当局も周知しており、[1]多くのACAMS会員の目にも留まったのではないだろうか。

世界各国・地域の金融当局が、ブロックチェーン技術の台頭に直面し、数年が経過している。FATFは「テクノロジーに対して中立」であるとしている[2] が、それは、例えば各金融サービスの基盤となっている技術に関わらず、「同種のリスクには、どのように同等の規制を適用するべきか」[3] という規制を検討しているとも言い換えられるだろう。多くの当局は、暗号資産による利便性を考慮しつつ、消費者保護やAML/CFT、拡散金融防止などの観点から、適切な規制を検討している。本稿では、暗号資産取引に際して求められる「トラベルルール」について、銀行送金とのFATF要件の違いを比較しながら説明したい。

なお、本稿に記載する内容のうち、意見・解釈に属するものは全て筆者のものであり、金融庁またはFATFの公式見解を示すものではない。

1. 本報告書の経緯

昨年実施された暗号資産交換業者にかかるACAMS Webinarにおいても、ACAMS会員からは、なぜFATFが特定業種のモニタリングを行うのかとの質問を受けた。これを説明するため、まずは本報告書がまとめられるに至った経緯を振り返りたい。

勧告15改訂の経緯

Figure 1:

How Recommendation 15 was revised[3,4]

Changes to FATF Standards (October 2018)	Changes to FATF Guidance (June 2019)	Changes to FATF methodology (October 2019)
* New definitions for virtual assets and VASPs * Revised Recommendation 15 * New Interpretive Note to Recommendation 16 on New Technologies (INR. 15)	* Revised INR. 15 * Release of new FATF guidance on a risk-based approach for virtual assets and VASPs	* New definitions for virtual assets and VASPs * Technical compliance: Revised R. 15 * Revised mutual evaluation methodology

INR. 15 and the "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (Guidance) both detailed AML/CTF requirements on VASPs, specifically that FATF member jurisdictions are required to impose adequate AML/CTF regulations on VASPs as per Recommendation 10-21 in INR. 15. This includes a requirement for wire transfers (i.e., Recommendation 16) which is referred to as the travel rule. FATF has been working to resolve the regulatory gap among jurisdictions and is calling on jurisdictions to develop legislation urgently to prevent the occurrence of "regulatory arbitrage." On balance, FATF explicitly states that it is technology-neutral body[5] in the Guidance.

At the February 2019 FATF Public Consultation and at the May 2019 FATF Private Sector Consultative Forum, some private sector and public sector officials expressed concern that VASPs do not have a technical solution nor infrastructure to implement the travel rule immediately. In light of that feedback, FATF decided to establish the Virtual Assets Contact Group (VACG, co-chaired by Japan and the U.S.), to monitor the amendment of laws in FATF member jurisdictions as well as the progress of the private sector in developing technical solutions to meet the requirements of the travel rule. The Report addresses the results of the VACG's monitoring activities.

Requirements for the travel rule

What are the requirements of the travel rule in virtual asset transactions, especially because the VASP sector argued that there was no technical solution nor infrastructure to immediately implement the travel rule? The following are the requirements for the travel rule in FIs to compare with the travel rule for VASPs.

Travel rule in FIs (Recommendation 16: Wire transfers)

According to the FATF Recommendations, "Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain."[6]

In Japan, the notification obligation under Article 10 of the Act on Prevention of Transfer of Criminal Proceeds is one of the laws that is applicable to Recommendation 16. Including "required and accurate originator information, and required beneficiary information" on wire transfers is generally fulfilled by the accurate inclusion of the required information when FIs transmit payment instructions via SWIFT and other payment systems.

Travel rule for virtual asset transactions (Recommendation 15 and INR. 15-7b)

The fact that the transfer of virtual assets is processed and recorded on a blockchain that can be technically viewed by an unspecified number of people makes the application of Recommendation 16 to VASPs practically difficult. It is impractical to have the names and addresses of customers recorded and published on the blockchain.

1. 2018年10月 - FATF基準の改訂[4] 。FATF基準の対象となる暗号資産（Virtual Asset）や暗号資産サービスプロバイダー[5] （Virtual Asset Service Provider。以下「VASP」）を明示。
2. 2019年6月 - 勧告15(新技術)解釈ノート[6] の改訂とガイダンスの公表。
3. 2019年10月- メソドロジー（相互審査手法）の改訂。

上記2「勧告15(新技術)解釈ノートとガイダンス」は、VASPに求められる詳細なAML/CFT要件を示したものである。例えばVASP は、勧告15解釈ノート7で、勧告 10から21のAML/CFT措置を求められている。ここにいわゆる「トラベルルール」として注目される、電信送金の要件である勧告16の通知義務が含まれる。FATFは、国・地域間での「regulatory gap」ひいては「regulatory arbitrage」の発生防止のため、各国・地域に対して、早急な法整備を求めたが、改訂に先立つ2019年2月の市中協議及び5月のPSCF（Private Sector Consultative Forum、民間セクターとの意見交換を実施）では、民間や当局者から「VASPがトラベルルールを直ちに履行する技術的手法が、存在しない」との懸念が複数寄せられた。

そこで、FATFは「コンタクトグループ（Virtual Assets Contact Group、以下VACG。日米による共同議長）」を設置し、FATF等メンバー国・地域による基準の実施や、民間セクターでのトラベルルールにかかる技術開発状況をモニタリングすることとした。VACGが、このモニタリング結果について取り纏めたものが、今般の報告書である。

2. 本報告書で挙げたられた「トラベルルール」の運用に係る課題

本報告書では、暗号資産に係るML/TFリスクや暗号資産市場の変化、各国での法整備状況もまとめられているが、本稿では、本報告書の第3節、第4節で挙げられた改訂FATF基準履行において確認された民間セクターでの課題、いわゆる「トラベルルール」に絞って説明したい。VAの取引では「直ちに履行する技術的手法が、存在しない」との声が上がったトラベルルールの要件とはどのようなものなのか。まずは金融機関におけるトラベルルールの要件を確認したい。

金融機関におけるトラベルルール「勧告16：電信送金（海外送金）」の要件

「各国は、金融機関が、正確な必須送金人情報、及び必須受取人情報を電信送金及び関連する通知文（related message）に含めること、また、当該情報が一連の送金プロセスを通じて電信送金、又は関連電文メッセージに付記されることを確保しなければならない。」とされ、本邦では犯罪収益移転防止法10条の通知義務がこれに当たる。この要件は、一般的に金融機関が支払指図をSWIFTや決済システムへ発信する際、必要情報を正確に含めることで履行されている。

Therefore, INR. 15 does not require the transfer of required customer information along with transaction data on the blockchain:

> "Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities."[7]

Due to the differences in technological information infrastructure, VASPs are not required to implement the same AML/CTF controls and system infrastructure used in FIs. VASPs are required to build and select a suitable infrastructure, which is currently undeveloped in VASP businesses. To understand those technological aspects deeper, the FSA's publication "Research on privacy and traceability of emerging blockchain-based financial transactions"[8] may help.

State of implementation by the private sector and public sector

Section three of the Report summarizes the private sector's response to the travel rule, including the status of the development of technologies for its implementation, and outlines how VASPs can implement the travel rule.[9] According to the Report, some argue that some of the information submissions required by the travel rule are already feasible if VASPs accept a cumbersome manual process. Since VASPs need to take measures to transfer virtual assets in the course of their business, the VACG focused on whether VASPs would be able to send a reasonably large volume of transactions to multiple destinations in an effectively stable manner.

Moreover, 55 jurisdictions and regional organizations responded to the survey conducted by the VACG, of which 32 jurisdictions self-reported that they had enacted the revised FATF Standards into law as of March 2020.[10] Seventeen jurisdictions out of 32 are refraining from compliance with the travel rule on the grounds that there is no holistic, instantaneous and secure technical solution for VASPs.

Challenges in travel rule implementation

The VACG conducted outreaches[11] in February and April 2020 to some Standard-setting bodies in the private sector, as well as some solution vendors that have published a white paper on the travel rule. Based on these outreach efforts, as well as the survey response and further input from the FSA, some common industry issues have been identified.

How to identify the counterparty VASPs

One of the biggest challenges of the travel rule is that the means of identifying the VASP that manages the beneficiary wallet has not been established. Since the transaction can be directly settled on the blockchain between wallet addresses alone, in the past, there was no need to worry about the VASP that manages the receiving wallet.

暗号資産交換業に適用されるFATF勧告15解釈ノート7b)

VAの移転は、不特定多数が閲覧できるブロックチェーン上で処理・記録されるため、依頼人や受取人を特定できない形でなされている。この特徴を踏まえ、VASPに対する改訂FATF基準の解釈ノートは、次のとおり、ブロックチェーン上ではなく別の形で、取引者情報を送付することを許容する記載となっている。

「各国は、発信元の VASP が、VA移転に関する正確な依頼人の必須情報と受取人の必須情報を確実に取得・保持し、上記の情報を受益者の VASP(略)に直ちに安全に提出し、当局の要請に応じて適切に利用できなければならない。」

VASPは、銀行で導入されているAML/CFT対策システムと同等のものを導入するのではなく、VASPに適するインフラの構築、選定が求められているのである[7] 。以上を踏まえ、本報告書で挙げられたポイントを見ていくこととしたい。

「報告書第3節:民間セクターによる実施状況」が指摘した点

報告書の第3節では、トラベルルールの実施に向けた技術やシステムインフラの開発状況を含む、民間セクターの対応状況をまとめている。詳細は報告書本文に譲ることとするが、本節における論点の一つは、VASPによるトラベルルールの履行手段について、「包括的で、即時かつ安全な技術的な手段」の有無であろう[8] 。トラベルルールで求められる情報の伝達は、煩雑な処理を厭わねばすでに実現可能な部分もあるとの意見があることも報告書は触れている。しかし、VASPは、業として暗号資産の移転を担っていることから、相応に大規模な取引情報を、複数の送付先へ、安定的に迅速に送付できる手段が開発可能かどうかということが、VACGのモニタリングでは注目された。

トラベルルールの論点等(報告書第4節:改訂FATF基準及びガイダンスにかかる課題を中心に)

トラベルルールの論点等について、いくつかの課題も特定されており、各々、以下の通り説明する。

- トラベルルールの導入にかかる論点

  VACGでは、本年2月及び4月に標準化団体及びトラベルルールにかかるホワイトペーパーを公表していたソリューションベンダーなどと意見交換を行った[9] 。本報告書では、これらや、各国サーベイ、金融庁からのインプットなどを踏まえ、業界共通の課題を挙げた。各々、報告書の項目に沿ってご紹介したい。

  1) 相手方VASPの特定方法
  トラベルルールの最大の課題の一つは、各々のウォレットを管理するVASPを特定する手段が確立していないことにある。依頼人・受取人とも、ウォレットアドレ

Compare a virtual asset transaction to a bank transaction. When the recipient's bank account number is known, there is no way to transfer the money if the name of the bank that holds the account is unknown. Based on this understanding, when someone wants to receive a money transfer, the sender must receive the bank's name (bank location and/or branch name as applicable), the name of the account holder, and the account number. Some use SWIFT business identifier codes (BICs) and other codes to specify the FI or legal entity to receive the money. In banking transactions, one only needs to look at the list of codes published by the central administrator to know which bank or legal entity corresponds with the specified code. For virtual assets, there is no such list of wallet addresses. The address is different for each type of virtual asset, and depending on the senders and receivers, the address could change from time to time. The revised FATF Standards require measures to address this.

The private sector also shared its pain points involving unregulated VASPs in the Report. Even if the counterparty VASP is identified, regulated sender VASPs would need to investigate such counter-parties from scratch, including (but not limited to) the VASP's registered location, whether it is regulated or not, if any regulatory action has been taken against it, and so on. Because this is burdensome for a single VASP, the private sector suggested publishing a list of regulated VASPs by each of the competent authorities as well as producing a global VASP list based on this information.

Peer-to-peer (P2P) transactions via private wallets

Although individual transactions that do not involve any VASPs are not subject to the revised FATF Standards, when a VASP deals with a private wallet, the VASP is subject to the revised FATF Standards. The private sector requested more detailed guidance on the expected control level. P2P transactions, which do not involve any VASPs, are not subject to the AML/CTF regulations under INR15, and thus represent a potential means to evade the regulations. Although there was no clear evidence of evasion of the regulation identified by FATF during the analysis, it is a subject of continuous monitoring. Further study of the market for P2P transactions is needed to identify the methods that each jurisdiction can take to mitigate risk as well as the clarification to the private sector.

Batch and post facto submissions and past transfers

INR. 15 states that "the originating VASPs (omitted) submit the above information to the beneficiary VASP (omitted) immediately and securely."[12] However, there is no guidance on how immediate it should be.

In this regard, the Report notes that the industry inquired as to whether the requirement could be met by sending a batch of data at the end of the day rather than at the time of each transaction and whether executed transactions should be addressed retroactively.

スのみで取引が完結するため、従来は各々のウォレットを管理するVASPを気にする必要性がなかったのである。

ここで、報告書に記載はないが、銀行取引と比較し説明させていただく。たとえ受取人の銀行口座番号を知っていても、その口座が「どこにあるか」を知らなければ振込む術はない。この共通認識が定着しており、送金を受けたい場合、先方には銀行名（場合によっては、銀行の所在国・支店名あるいは支店番号）と口座名義を口座番号と共に伝えるだろう。SWIFTコード等で受取金融機関や事業法人を指定することもあるが、その場合でも、中央管理者が公表するコード一覧さえ見れば、どの銀行・事業会社か判別できる。これに対し、暗号資産のウォレットアドレスでは、そのようなリストはない。暗号資産の種別・送付・受取ごとにアドレスが異なるのみならず、都度変更もあり得る。改訂FATF基準の履行は、これら要素への対処策が必要となる。

報告書内容に戻るが、民間セクターからは、無登録の事業者への送付防止も課題とされた。受取人・依頼人のVASPが判明した場合も、現状ではそのVASPの素性（所在国・金融監督当局・登録・免許有無等）は、依頼人のVASPが一から調査する必要がある。民間セクターからは、各国当局による監督下VASPのリスト公表や、それを基にしたGlobal VASP Listを作るという案が寄せられた。

2） Peer-to-peer（P2P）取引
VASPが一切関与しない個人間取引については、改訂FATF基準の対象外であるものの、VASPが（VASPを経由しない）プライベート・ウォレット等と取引する際、VASP側には、改訂FATF基準が適用される。この際に求められる対応については、より詳細なガイダンスを求める声がある。

なお、VASPを一切介さないPeer-to-peer（P2P）取引については、改訂FATF基準で、AML/CFT規制の対象外であるが故、規制回避手段となる懸念がある。今回の分析時点では、規制逃れの動きを示す明確なエビデンスは確認されていないものの、当局間でも懸念事項として認識されており、今後も継続的な注視対象とされた。P2P取引の市場調査（規模、シェア）、ML/

Interoperability of systems, and data compatibility

Some say that a "SWIFT-like" infrastructure is needed as a technical solution to the travel rule. However, FATF does not necessarily call for the introduction of a unified "SWIFT-like" system. Indeed, many are expecting multiple solutions to line up alongside each other. Particularly with the staggered effective dates of legislation, it will be difficult to consolidate the needs of VASPs from different jurisdictions into a single system. Several proposed solutions on the infrastructure side are being built globally. Although the control specifications vary, only screened VASPs will use such infrastructure, so the need for due diligence on the counterparty in the transaction phase will be eliminated. In addition, it seems that other industry working groups are discussing the development of a Wolfsberg questionnaire for effective VASP due diligence.

With that in mind, the practical and effective operation of the travel rule requires compatibility between multiple parallel infrastructures.[13] To ensure such compatibility, a working group was established by virtual asset sector stakeholders and a common data item format was developed across industry associations and solution vendors.[14] A multifaceted study will continue to be conducted to make those system interoperable.

The sunrise issue

From a travel rule standpoint, it is unclear how a regulated VASP should treat VASPs in unregulated jurisdictions and this problem could continue until the appropriate AML/CTF regulations have been introduced across all concerned jurisdictions; the VACG calls this situation the "sunrise issue." VASPs should be aware that the approach to this issue may vary among jurisdictions. Some regulators take a phased approach, where they implement registration and/or licensing to VASPs, then implement the travel rule after a regulator becomes aware of solutions that handle required data in a "holistic, instantaneous and secure manner" within their jurisdiction. Further, the VACG highlighted the need for interjurisdiction coordination. Cited in mind was a VASP with global footprints, with no headquarters or control functions in any particular jurisdiction which is a business model seldom seen in FIs. The "sunrise issue" points to VASPs and FIs; the challenge at regulated VASPs and FIs will be to identify the risk factors they shall review when they start new business relationships with a VASP, while apparently avoiding de-risking behavior. Although the above mentioned example could be rare, VACG members started the discussion to have a more coordinated approach, including the concept of information sharing and coordination between authorities across jurisdictions. Over the coming year, FATF will continue the discussion on this matter. Thus, the private sector should keep a close eye on what the authorities are doing.

TFリスク低減のために各法域が採ることができる手法及び現在のFATFガイダンスの十分性については、更なる検討が必要としている。

3）　バッチ処理や事後処理による情報送付
勧告15解釈ノートには、「発信元の VASP が（略）直ちに安全に提出」とあるが、どの程度「直ちに」行うべきかのガイダンスはない。この点、本報告書は、業界からの照会事項として、取引の都度ではなく終業後に一括して送付することで要件を満たせるか、既に実行済みの過去の取引を遡って対処すべきか、といった点を挙げた。

4）　システムの相互運用性（データ互換性）
トラベルルールの技術的解決策については、「SWIFTのような」インフラの構築が必要と形容されることも多い。この点、FATFは必ずしも「SWIFTのような」単一システムの導入を求めていない。現在、様々なトラベルルールの技術的解決策が開発中であり、VACGも複数のソリューションが併存する状況を予想している。[10]

筆者が業界団体などが主催するセミナーなどで確認した範囲では、現在、グローバルにみて複数の情報授受インフラが構築中である模様。コントロール仕様は異なるが、審査を経たVASPのみに利用を限り、暗号資産の移転段階では相手方VASPのデューデリジェンスを不要とするスキーム、デューデリジェンスに資するよう、VASP向けのWolfsberg questionnaireの策定といった動きもあるようである。

このようにソリューションが併存する場合、FATF基準の実効的な履行には、併存する複数インフラ間での互換性が必須となる。こうした互換性を確保するため、暗号資産業界[11]でもワーキンググループが立ち上がり、業界団体、ソリューションベンダーを跨いだ、共通のデータ項目フォーマットが策定された[11]。今後もシステムの相互運用を可能とすべく、多面的な検討が続くと思われる。

5）サンライズ問題
規制未導入国のVASPをトラベルルールの実施上どのように扱えば良いかが不明確な状態が、当該国の規制導入（例えるならば、サンライズ）まで継続することを指している。一

Specific wording issues in the glossary of terms in the FATF Standards

INR. 15 sets out the travel rule for VASPs, using terms from the Interpretive Note to Recommendation 16 in part. For example, clarification was sought from the private sector on how to read “required originator information” in a VASP context. Similarly, so-called stablecoins are not explicitly covered by any FATF guidance, although FATF announced that so-called stablecoins are covered by FATF Standards either as a virtual asset or as a traditional financial asset.[15] Classified in either categories in a jurisdiction, a regulated entity needs to implement travel rule control for so-called stablecoins as well. Risks involving so-called stablecoins that are not currently being addressed include 1) P2P transactions; 2) regulatory arbitrage due to the regulatory gap; and 3) decentralized governance structure (e.g., those without a central government entity such as the Libra Association, which is behind the Libra stablecoin), all of which FATF intends to develop guidance on in the future.[16]

Proposed next steps in the second 12-month review

The Report concluded that the VACG will conduct the second 12-month review to monitor the progress in the virtual asset sector and listed the following five action items for next steps:

1. Conduct a second 12-month review (due June 2021)
2. Revise FATF guidance for further details on the travel rule, P2P transactions and stablecoins
3. Release red flags for virtual asset transactions (planned to be released October 2020)
4. Facilitate dialogue with a broader range of virtual asset sector stakeholders (including technical and academic experts) with a focus on monitoring the progress of travel rule implementation
5. Strengthen international cooperation between supervisory authorities

In many jurisdictions, the virtual assets sector is a young industry. Thus, the VACG has been promoting collaboration among regulators and dialogue with the virtual sector with an eye toward effective AML/CTF regulatory application. VASPs, vendors and other private sector stakeholders should be encouraged to collaborate further with the VACG on its activities in the future.

Arisa Matsuzawa, CAMS, deputy director, AML CFT Policy Office, Strategy Development and Management Bureau, Financial Services Agency, Japan, Arisa.matsuzawa@fsa.go.jp

Please note, any opinions and interpretations in this paper are those of the author and do not represent the official views of the FSA or FATF.

事業者の立場からも、規制導入済みの事業者として、規制未導入国に所在するVASPとの取引方針やデューデリジェンス手法の検討は課題であろう。今後FATFが策定するガイダンスでは、この対応についての記載も見込まれる。

また、登録・免許対象となるVASPの捉え方についても、懸念点があることは挙げられている。これは例えば、「国際的な業務展開があるものの、特定の国・地域に本部機能を置かないVASP」など当局間の連携が必要な事例があり、国・地域を跨いだ当局間の分担や連携の在り方は、FATFでも重視されている。民間セクターにおいても、こうした当局の動きは、注視しておくべきであろう。

6）FATF基準上の用語解説

VASPのトラベルルールを定める勧告15・解釈ノートの記載は、一部、勧告16の解釈ノートの定義を用いている。例えば、“required originator information”はVASPでどう読み替えるべきか、民間セクターからは、ガイダンスでの明確化が求められた。これに加え、いわゆるステーブルコインについても、ガイダンスでは更なる解説が見込まれる。FATFは、いわゆるステーブルコインはFATF基準の対象であると明示しており 、暗号資産と見做すか、[12]伝統的な金融商品と見做すかは各当局にゆだねられているものの、民間セクターが取り扱う際にトラベルルールなどの対応が必要なことに変わりはない。ステーブルコインに関する現在対処できていないリスクとして、①仲介業者を通さないP2P取引、②規制が不十分な法域の存在（規制裁定）、③分散型ガバナンス構造（例：リブラにおけるリブラ協会のような中央ガバナンス主体となりうる存在がないもの）を挙げ、今後FATFとしてのガイダンスを作成するとしている 。[13]

3. 第2期12か月レビューが目指すもの（「報告書第5節：今後の活動」）

本報告書第５節では、VACGがモニタリングを継続することが報告され、今後の活動項目が挙げられた。

a) 2期目の12カ月レビュー実施（2021年6月期限）

b) FATFガイダンスの改訂

第４節も踏まえ、トラベルルール、P2P取引、ステーブルコイン等について更に詳細なガイダンスを作成。

c) VA取引にかかるレッドフラッグを公表（2020年10月）

[1] "Embedded supervision : how to build regulation into blockchain finance," *Bank for International Settlements*, September 2019, https://www.bis.org/publ/work811.pdf

[2] "12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers," *Financial Action Task Force*, June 2020, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html

[3] "Outcomes FATF Plenary, 17-19 October 2018," *Financial Action Task Force*, October 19, 2018, http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html

[4] "Public Statement – Mitigating Risks from Virtual Assets," *Financial Action Task Force*, February 22, 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html

[5] "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," *Financial Action Task Force*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

[6] "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations," *Financial Action Task Force*, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

[7] Ibid.

[8] "Research on privacy and traceability of emerging blockchain based financial transactions," *Financial Services Agency and the Mitsubishi Research Institute, Inc.*, March 20, 2019, https://www.fsa.go.jp/policy/bgin/ResearchPaper_MRI_en.pdf

[9] "12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers," *Financial Action Task Force*, June 2020, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html

[10] This Report is based on the self-reporting of countries, not the results of the FATF review.

[11] At this meeting, FATF did not endorse any private sector products. Please take note that objective technical constraints, challenges identified by the private sector, and market trends were discussed at the meeting.

[12] "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations," *Financial Action Task Force*, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

[13] Looking at national settlement systems (e.g., BOJ-Net, Fedwire, MAS net) and securities settlement (e.g., DTC, FICC), there are multiple mechanisms coexisting depending on the currency or product. It also recalls the transition of securities settlement systems through consolidation and merger.

[14] "interVASP Messaging," *interVASP Messaging*, https://intervasp.org/

[15] "Money laundering risks from 'stablecoins' and other emerging assets," October 18, 2019, http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html

[16] "FATF Report to G20 on So-called Stablecoins," *Financial Action Task Force*, June 2020, http://www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html?hf=10&b=0&s=desc(fatf_releasedate)

d) トラベルルール導入の進捗モニタリングを主眼に、より広範なVAセクター関係者（技術者、学術有識者含む）との対話を促進する。

e) 監督当局間の国際協力の強化

多くの法域でVAセクターは若い業界であるところ、VACGでは、ML/TFに対する効果的な規制の適用を念頭に、当局間の連携とVAセクターとの対話を進めてきた。今後もVACGの活動について、VASPやベンダーをはじめとする民間セクター関係者には、更なる協力をお願いしたい。

松澤　亜里沙、CAMS、金融庁総合政策局マネーローンダリング・テロ資金供与対策企画室室長補佐

[1] https://www.fsa.go.jp/inter/etc/20200701_2.html

[2] http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf　パラ19 b), 49、119。

[3] "BIS Working Papers No.811 Embedded supervision: how to build regulation into blockchain finance" https://www.bis.org/publ/work811.pdf

[4] http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html

[5] なお、資金決済法では「暗号資産交換業者」としており、厳密な定義は各々原典を参照されたい

[6] 市中協議として公表された解釈ノートドラフト：http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html

[7] なお、金融庁が2019年3月に公表した「ブロックチェーンを用いた金融取引のプライバシー保護と追跡可能性に関する調査研究」は技術面に焦点を当てており、AML/CFT対応へも示唆を含んでいるところ、本分野にご興味のある方はご参照いただきたい。

[8] 本報告書パラグラフ39、42

[9] 本会合で、FATFが私企業の製品を公認したのではなく、客観的な技術制約や、民間セクターが認識した課題、市場動向につき意見交換する場であった点、留意願いたい。

[10] 各国の決済システム（例：BOJ-Net, Fedwire, MAS net）や証券決済（例：DTC、FICC）のように、取扱通貨・商品により複数の決済システムが併存する例や、ユーロクリア、クリアストリームといった、統合・合併がなされた例もある。

[11] https://intervasp.org/

[12] http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html

[13] 本報告とは別に、FATFはいわゆるステーブルコインにかかる分析レポートを公表し、G20へ提出予定である 。詳細は当該レポートを参照されたい。http://www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html?hf=10&b=0&s=desc(fatf_releasedate)

Datuk Seri Azam Baki: Pulse on AFC in Malaysia

ACAMS Today interviewed Datuk Seri Azam Baki, chief commissioner of the Malaysian Anti-Corruption Commission (MACC). Azam Baki began his career at the Anti-Corruption Agency (ACA) in 1984, now the MACC, as an assistant investigation officer. Throughout his service at the ACA, he carried out duties as an investigation officer, intelligence officer, prosecuting officer and he took part in community education activities. He graduated with a diploma in electrical engineering from Universiti Teknologi Malaysia, a degree in law (Jurisprudence) from the University of Malaya, and a master's degree in business operation from Asia e University. Azam Baki has served the MACC for over 35 years. Finally, he was a pioneer in the forfeiture of properties system under the Anti-Corruption Act 1997, the MACC Act 2009 and the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2010 (AMLATFPUAA).

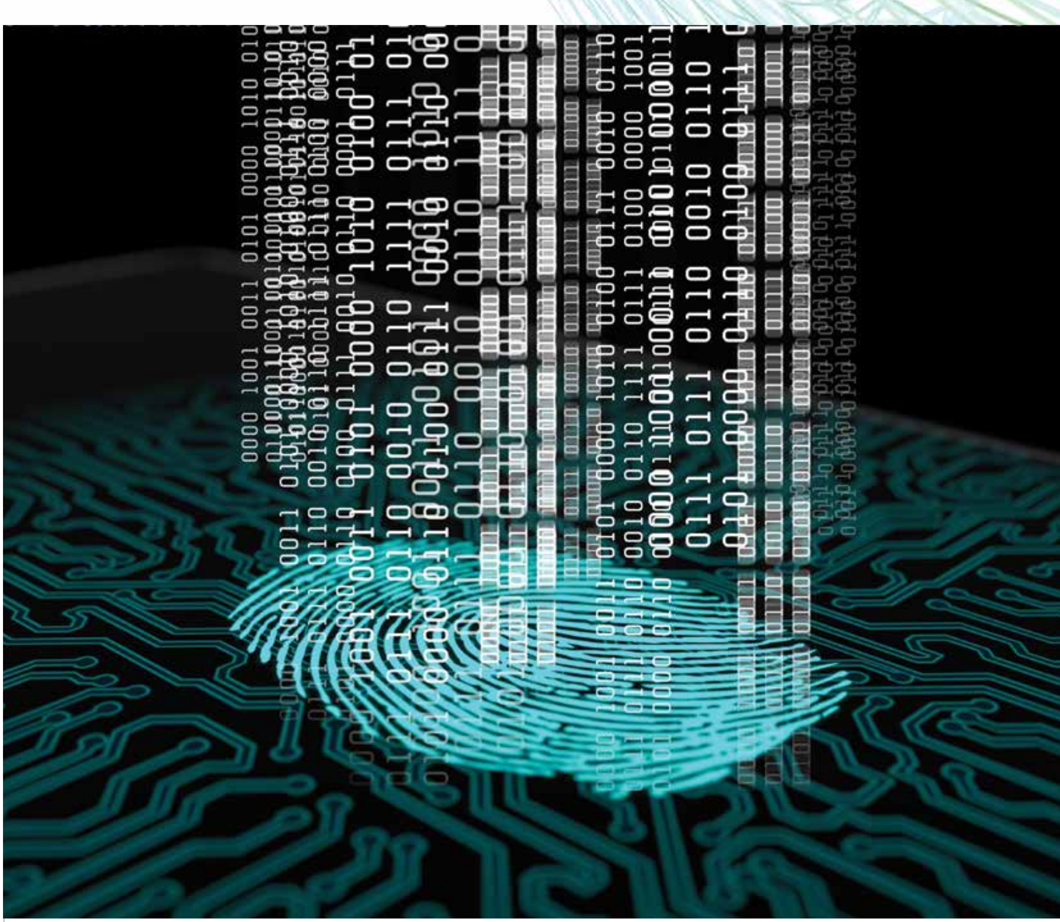
ACAMS Today: **You have held various key roles with the MACC for more than 35 years and now you are the MACC chief commissioner. How has crime and corruption changed in Malaysia throughout your career?**

Datuk Seri Azam Baki: When I joined the agency in 1984, it was still known as the ACA. At that time, the ACA positioned itself as a specific body designed solely to investigate corruption cases. Then it went through changes that better highlighted the government's efforts to strengthen the agency's powers and made it more independent until we finally had our own Anti-Corruption Commission in 2009.

In line with economic progress over the decades, the types of corruption offenses under investigation in our country have evolved from small corruption cases to those that are more complex and syndicated in nature.

In recent years, corruption is coupled with money laundering activities, which means there is a need for greater improvements in our investigative techniques. Hence, forensic approach, financial tracking and asset tracing, intelligent-based investigation and forfeiture of criminal assets (among others) have become highly relevant and are now being used and practiced in the MACC.

AZAM



The government enacted the AMLATFPUAA as a strategic national response to the Financial Action Task Force's (FATF) Recommendations on how to fight money laundering and terrorist financing activities. We have found that crimes are now becoming more transnational and globally linked. Therefore, the Mutual Assistance in Criminal Matters Act 2002 was enacted to complement cross-border investigation and recovery of criminal assets abroad.

I do believe there have been many positive changes and great improvements in the MACC to ensure it remains relevant and able to withstand the evolution of corruption offenses both in our country and globally. I have been with the MACC long enough to see the internal changes and I assure you that our main focuses have always been and will remain eradicating corrupt practices within our shores, educating the masses on the importance of reporting corrupt practices and abstaining from acts of corruption. We are always watching!

AT: You recently passed 100 days since being appointed chief commissioner. What are your priorities for the MACC for fiscal year 2020-2021?

DSAB: I believe, along with my fellow officers, the MACC has to be aggressive and highly responsive to corruption and misuse of power in our country. For example, in 2019 we initiated and prosecuted a number of high-profile cases, forfeiting 1.29 billion ringgit ($3.07 billion) in proceeds of crimes.

The global economic downturn caused by the COVID-19 pandemic has inevitably impacted the domestic economy. Whilst efforts to boost the domestic economy as well as international trades and commerce are at play, it is pertinent that any leakages in the economy are dealt with appropriately.

For the fiscal year 2020-2021, the priorities for the MACC remain in these three key sectors: law enforcement, public procurement and grand corruption cases. These are critical areas in the national agenda for fighting corruption and for driving Malaysia toward being a developed and high-income nation.

The fight against corruption, particularly in these three key sectors, has been the focus of previous national initiatives like the National Integrity Plan, Vision 2020, the Government Transformation Programme and others. The most recent commitment has been well documented in the National Anti-Corruption Plan (NACP) 2019-2023, which is comprised of 115 initiatives in the areas of governance, integrity and anti-corruption, of which the MACC primarily leads 12.

AT: Is Malaysia achieving the right change of culture (in terms of corporate governance, law enforcement and public sector administration) under the NACP?

DSAB: On July 6, 2020, at the prime minister's department monthly gathering, the Malaysian prime minister said, "That is why the Anti-Corruption Plan that was agreed upon during the previous administration will continue." He concluded, "We want to ensure that all matters pertaining to administration will be conducted according to the rule of law."

The anti-corruption plan mentioned by the prime minister was the NACP. The NACP 2019-2023 was introduced on January 29, 2019, as an anti-corruption policy with the goal of making Malaysia corruption-free and a nation that exhibits transparency, accountability and integrity. This plan was designed in tandem with Article 5 of the United Nations Convention Against Corruption.

The NACP set six priority areas that are core pillars in the fight against corruption: political governance, public sector administration, public procurement, legal and judicial, law enforcement and corporate governance. The Governance, Integrity, and Anti-Corruption Centre (GIACC), which is set up under the prime minister's department, is critical in coordinating multi-actor contributions toward accomplishing goals under this NACP.

Since 2019, all 115 initiatives outlined under the NACP have been monitored regularly by the GIACC for progressive implementation. They are also reported periodically to the prime minister under the mechanism of the Cabinet Special Committee on Anti-Corruption (JKKMAR). Through this mechanism, these initiatives would also withstand reviews and improvements to ensure there are implementable end outcomes.

I have trust in the genuine spirits behind the NACP and I am committed to drive the MACC toward accomplishing the 12 initiatives it was entrusted to spearhead. I also ensure that the remaining initiatives driven by other ministries/departments/agencies have the necessary support from the MACC. I have observed the continuous commitment and dedication to the highest level from most ministries, departments and agencies in translating these initiatives into reality.

The introduction of the NACP by the government evidently contributed toward Malaysia's improved Corruption Perceptions Index score in 2019. Malaysia now ranks 51st among 180 countries with 53 points, compared to ranking 61st in 2018 with 47 points. So, Malaysia is really on the right track.

AT: Do you feel that the MACC is ahead of the curve or behind the curve in delivering its message out to financial crime audiences?

DSAB: Corruption typologies in Malaysia are changing due to the development of our nation's economic environment. Malaysia has undergone several law reforms to strengthen its anti-corruption enforcement.

The types of corruption cases that we are seeing now both domestically and internationally involve complex transactions. There is fraud, financial statement manipulation to hide illegal proceeds, and a sharp increase in the usage of financial institutions outside Malaysia to facilitate the ill-gotten proceeds and others. That is why I am passionate about ensuring my officers always have the latest technologies and investigating techniques, skills and tools. We do not want to be in a situation where we are lacking in skills—whether they be financial, accounting or otherwise—when we are investigating high-profile or high-scale cases.

Financial crimes have now transcended across borders, so it has become a challenge for us to trace assets inside and outside the country as it involves a large scale of assets. Current examples of cases on trial are the 1Malaysia Development Berhad and SRC International Sdn Bhd cases. They are high-scale cases involving high-profile figures, which proves that we too need financial experts on our end to deal with financial analysis.

I have trust in the genuine spirits behind the NACP and I am committed to drive the MACC toward accomplishing the 12 initiatives it was entrusted to spearhead

The aforementioned reasons are why Malaysia requires the new law on corporate liability enacted. The government and lawmakers had enacted Section 17A under the MACC Act 2009 in 2018, which has now been gazetted and was implemented in June 2020, and has resulted in a law that can hold commercial organizations liable if their employee or associate is found to be involved in corruption.

I believe the MACC is ahead of the curve, as can be seen by our successes in completing and prosecuting many high-profile and public interest cases for the past years. Our focus will continue on combating corruption and ultimately achieving the Malaysians' aspiration for a country free of corruption.

AT: Does the financial community need to strengthen whistleblower protection?

DSAB: One way to detect and deal with improper conduct is through information provided by whistleblowers. Generally, a whistleblower is an insider of an organization (e.g., employee, consultant, vendor) who reports improper conduct that has occurred within that same organization.

In an effort to encourage whistleblowers to come forward with information on any alleged improper conduct, the Whistleblower Protection Act 2010 was enacted to provide a safe avenue to encourage disclosures of such alleged improper conduct to the relevant authorities in good faith, by protecting their identities, providing them with immunity from civil and criminal proceedings, and protecting them from detrimental action.

We at the MACC would in many instances rely on the information specifically given by whistleblowers that inform enforcement agencies of a corrupt act or on organized crime. Thus, there is a need for financial communities to strengthen their whistleblower mechanisms.

Whistleblower information and protection are very important to the MACC and that is why strengthening laws and providing more protection to whistleblowers will always be supported by the MACC.

In addition, the act itself must be seen by the public to be independent. We are looking at putting in a proposal to the prime minister and the prime minister's cabinet to have an independent authority be established to oversee the act, whistleblower protection provisions and mechanisms.

To increase public confidence in making disclosures, a trained unit specialized in handling whistleblower disclosures will enable the proper reception and handling of sensitive disclosures.

AT: You have driven very successful investigations at the MACC. How was the investigative method adapted to new technology and new techniques?

DSAB: Due to growing complexity in the modus operandi of corruption cases, the MACC has adopted a proactive approach in our investigation process. One of the techniques in the proactive approach is intelligence-based investigation (IBI). There are two types of cases that need IBI: undercover investigations and high-profile cases. IBI is a methodology for intelligence gathering that will be used in these investigations. By conducting IBI, an investigation can be more effective and efficient by creating a more concentrated scope of investigation and identification of possible obstacles that may arise.

To avoid being caught, the perpetrators are resorting to the use of technology and sophisticated modus operandi in executing their plans. To always be ahead, the MACC is committed to always improving its capability, competency and capacity in terms of human resources as well as investigation tools. We equip our forensic technology division with the latest gadgets and trainings from certified experts. We send our officers to various trainings in financial, accounting, engineering and other areas to improve their knowledge and skills.

In the future, we want to be able to confiscate the virtual assets and also forfeit them—same as any other currencies that are being used

In addition, we also recruit more professionals to be our officers in order to improve fighting corruption. We have our own financial analysis division to do the tedious analysis work, go through financial records, and uncover what is being hidden in the numbers. Their involvement is equivalently crucial at every part of the investigation, from information gathering to the launch of the open investigation.

AT: What are your thoughts on the development of crypto and virtual assets and the advancement of digital banking as new vehicles for corrupt practices?

DSAB: Recently, the Securities Commission (SC) was appointed as the regulator for cryptocurrency industries in Malaysia with the enforcement of the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 under the Capital Markets and Services Act 2007. The SC has now registered three recognized market operators to establish and operate digital asset exchanges in Malaysia.

The MACC as an enforcement agency is always aware of the latest trends in corruption and money laundering activities in Malaysia. In terms of virtual assets, we will be working closely with the SC as the main regulator for virtual asset service providers to detect and prevent any potential corrupt practices using these platforms. On the other hand, our officers will be equipped with necessary training on virtual assets, how it works and the possible risks that may arise. We will also look into the need to strengthen our current law to cater to virtual asset transactions. In the future, we want to be able to confiscate the virtual assets and also forfeit them—same as any other currencies that are being used.

AT: Can you foresee any opportunities to improve training or education for the AML and anti-corruption community?

DSAB: As mentioned earlier, virtual assets are one of emerging typologies in money laundering and anti-corruption. It

is becoming more significant with the growth of cybercrime. Online gambling, cryptocurrency and casinos are some examples of the new platforms perpetrators use to launder their money and pay illegal proceeds. As an AML and anti-corruption community, we need to enhance our knowledge on the modus operandi of these virtual assets through trainings and exposure to the real-life situations.

Anti-corruption trainings must include all potential threats and high-risk areas of corruption, abuse of power and money laundering. New methods and modus operandi for payment of illicit purposes need to be updated according to the rapid development of technology as well as the fluctuation in global politics and economy. This is where collaboration between regulators, reporting institutions and enforcement agencies is very much required.

We must also not forget the role of professional communities. We need their support through their active research activities, studies and statistical reporting, which will help us in determining the loopholes, planning the preventive mechanism, as well as bringing all the players closer in the fight against corruption.

All reports relating to recent corruption and money laundering typologies, studies and surveys compiled by authorities and independent bodies such as FATF and the Asia/Pacific Group on Money Laundering should be made available to financial firms, so they are exposed to the methods of potential criminals, thus enabling appropriate action be taken to prevent occurrence or early detection to minimize repercussion or impact to anti-corruption risks.

AT: Are there any new areas that need to be added to a financial firm's anti-corruption trainings?

DSAB: Commercial crime always involved complex layering of accounting records in order to hide the illegal transactions. It is very crucial to have a team of professionals and experts to scrutinize all the records and uncover the modus operandi through financial records trailing, forensic accounting and financial statements analysis.

Besides that, due diligence process during first engagement with the public is crucial in eliminating the risk of corruption and money laundering. Regulators and enforcement agencies will be depending on these reporting institutions to trigger any red flags on suspicious transactions.

Another area that is becoming more significant is the use of beneficial ownership to cover illegal practices. Companies are being used to cloud the eyes of enforcement agencies and to legalize its illegitimate financial gains. The Malaysian Companies Act 2016 was amended several years ago with a new provision granting the power to a company to inquire into the beneficial owner of the shares in a company was inserted.

The MACC is also in the midst of preparing the paperwork for a new provision in our MACC Act 2009 to criminalize the use of beneficial ownership as a vehicle for corrupt practices. We have full support from the government in this matter and we will coordinate with all the relevant parties to establish a monitoring mechanism to ensure a transparent disclosure of beneficial ownership.

AT: From your perspective, where are the hotspots or trends in corrupt practices that need attention across the Asia-Pacific (APAC) region?

DSAB: The APAC region is known for its diversity in terms of culture, religion and politics. Crimes that are always intertwined with corruption (such as human trafficking, smuggling and money laundering) will continue to be the main focus in the anti-corruption agenda of this region.

In October 2019, the MACC had exposed a series of videos that showed smuggling activities and a security breach at the Thailand-Malaysia borders. This kind of evidence is very much needed and must be addressed as it is jeopardizing the economies and security of both countries involved.

I think there is a need to have better collaboration between members of the region in terms of understanding and response toward informal and formal bilateral assistance. We need to find ways to improve information sharing and evidence gathering across the region in cases that involve multinational jurisdictions. To achieve this, each country must have a shared vision in fighting corruption regardless of any differences in ideology and politics.

Interviewed by: Dr. William Scott Grob, CAMS, AML director, ACAMS, Hong Kong, wsgrob@acams.org

Aaron Lau, CAMS-Audit, CAMS-FCI, AITLAU Management Services, Kuala Lumpur, Malaysia, aaron@aitlau.com

ADVERSE MEDIA SCREENING NEEDS AI TRULY, DESPERATELY AND IMMEDIATELY

This article will not begin with a story that emphasizes how hard adverse media screening (AMS) currently is—the reader is likely well-aware of the difficulty. It will, however, dissect why it is so hard and why artificial intelligence (AI) is the hero for which AMS has been waiting.

While in most cases AI as a hero is a tattered-half truth, in this case, it is beneficial for a vast majority of examples discussed. And for those who work in AMS (was it mentioned how hard it is?), that is cause for celebration.

Why AMS is hard

Confusing compliance

The regulatory guidelines senior bank managers have been given on AMS are not exactly clear–or easy to execute.

In a recent set of draft guidelines, the European Banking Authority gave AMS the following rough definition:

> "Are there adverse media reports or other relevant sources of information about the customer, for example are there any allegations of criminality or terrorism against the customer or the beneficial owner? If so, are these reliable and credible? Firms should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. Firms should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing."[1]

Unpack this statement for a moment. What does the term "relevant sources" mean for a financial institution? Does it mean the AMS data providers in the marketplace? Does it mean mainstream media? What is the definition of reliable and credible? Does this exclude small, independent crusading journalists who often break financial crime stories first? What do quality and interdependence mean?

Things do not get any easier for bankers across the pond. The Financial Crimes Enforcement Network's Customer Due Diligence Requirements for Financial Institutions stated, "Covered financial institutions should also develop risk-based procedures to determine whether and/or when additional screening of these names through, for example, negative media search programs, would be appropriate."[2] This guidance is even more challenging to define within a program.

As with any vague set of instructions, the outcome is inconsistent application. These inconsistencies can exist both between and inside firms as different business units may set their risk appetite according to the resources they have at hand to address the issue.

For any bank's senior leadership, that lack of consistency should be worrying. They have good reason to be kept up at night by convoluted risk exposure and the real potential of a crucial miss, leading to regulatory scrutiny, reputational risk and potential fines.

Boiling the ocean with a kettle

The nighttime anxiety bankers are feeling is compounded by two additional problems: the exponential growth of "relevant" data and the manual nature of the current AMS process.

Much of the data integral to the AMS process is unstructured. It is not in columns or rows–things that are easily analyzed by computers. It is largely written text, information that has traditionally required the human touch to analyze effectively. In addition, the volumes at which this data is being produced are extraordinary; there are 2.5 quintillion bytes of data created each day at the current pace and 90% of the data in the world was generated over the last two years alone.[3]

This would not be so bad if AMS programs were using the latest analytical technologies, but, put plainly, they are not.

The current methodology? Often, it is just an analyst and Google.[4] The analysts enter a variety of searches with names and keywords. This produces a veritable mountain of results. They comb through the documents and articles, one by one, checking each for content and credibility. Some of it will be irrelevant or not credible, while some of it will identify key risks in firms' customer bases. In any case, it is tedious, exhausting and error-prone work.

Given the problems and the process, is it any wonder that chief compliance officers and chief risk officers struggle to be confident that they have a handle on all the risks?

Why AMS does not have to be so hard

Natural language processing (NLP), the branch of AI that focuses on the analysis of human language, is particularly suited to the challenges of AMS.

Search engines like Google, Bing and others are built on NLP. But as powerful as they are, those tools are generic, designed for the needs of the average user. What analysts need is a tech platform built to their specific requirements, and such an application is fully within the art of the possible. All the NLP technologies needed to create it—such as categorization and document similarity—exist and are in widespread use.

A modern AMS solution consumes numerous open-source intelligence inputs. The content is analyzed and categorized based on the relevant sanctioned activities using a domain-specific categorization algorithm.[5] Using semantic similarity to compute similarity between documents, an NLP model can detect the meaning of linguistic content, removing duplicate content and filtering out information without a sanctioned activity.

High-risk content is detected using semantic similarity and sentiment analysis. Semantic similarity differentiates between specific financial crimes, both in usage and content. "Perpetrated a fraud," for example, is far cry from "victim of fraud." Sentiment analysis detects the tone of the text, identifying when a contact is associated with a highly negative piece of information. Strong positive hits are prioritized for analyst review, and this allows humans to perform high-value tasks instead of hours of trawling and grunt analyses.

This approach provides the consistency that bank leadership wants–AMS would be handled in the same way with the same risk rules across all the business lines–while addressing the concerns of regulators:

- Relevance can be defined by the firm without losing the ability to spot critical outliers.
- Credibility, quality and interdependence can be algorithmically defined and refined.

AMS: A problem that AI can actually solve

Banks need to move beyond brute keyword searching and manual analysis. Despite how glossy tech marketing can be, there are a million things AI cannot do, but AI can do AMS.

The technology is not an alpha or a beta. It is fully mature and has been used in many other domains, specifically intelligence, for years. So, the question is not feasibility. It is just execution.

Steve Cohen, COO, Basis Technology, Cambridge, MA, USA, stevec@basistech.com

[1] "Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The Risk Factors Guidelines"), amending Guidelines JC/2017/37," *European Banking Authority*, February 5, 2020, https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2020/Draft%20Guidelines%20under%20Articles%2017%20and%2018%284%29%20of%20Directive%20%28EU%29%202015/849%20on%20customer/JC%202019%2087%20CP%20on%20draft%20GL%20on%20MLTF%20risk%20factors.pdf

[2] "Customer Due Diligence Requirements for Financial Institutions," *Federal Register*, May 11, 2016, https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf

[3] Bernard Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, May 21, 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#5c192ada60ba

[4] Sujata Dasgupta, "Adverse media screening: a key pillar of financial crimes compliance," *Fintech Futures*, June 29 2020, https://www.fintechfutures.com/2020/06/adverse-media-screening-a-key-pillar-of-financial-crimes-compliance/

[5] For instance, the 22 predicate offenses contained within the Sixth AML Directive (6AMLD).

The new ACAMS brand: The journey

The idea of improving the world while also changing how you interact with it is best articulated by Leo Tolstoy, who famously said: “Everyone thinks of changing the world, but no one thinks of changing themselves.”

ACAMS decided it wanted to do both. With help, guidance and support from a global financial crime prevention community peppered across 175 countries and jurisdictions globally, we embarked on the mammoth task of affecting positive internal and external change. The task was challenging, as our members around the world relate to and are very passionate about the ACAMS brand. What added complexity to the project canvas was the parallel task of a full website redesign for ACAMS’ global membership base. This process entailed an improved user experience, with streamlined training being adapted for nine different languages.

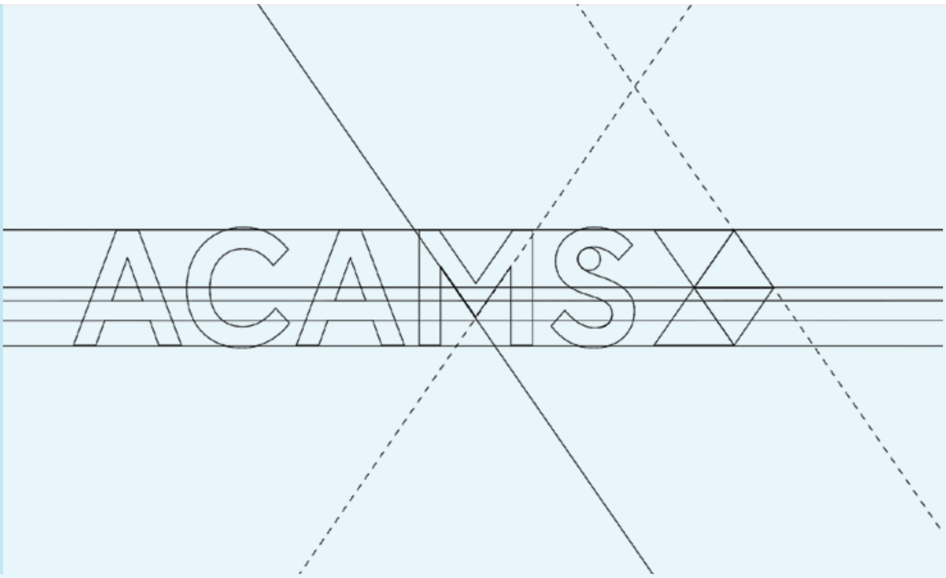
The launch of the new ACAMS brand follows over 100 hours of interviews and meetings with members, partners and employees across six continents, nearly a dozen rounds of testing with focus groups and the consideration of more than 165 logos and design directions.

I was incredibly honored and humbled to be entrusted with the responsibility of leading this initiative that began in January 2019. What was clear from the start was that we needed to heed feedback from our members indicating that we needed a world-class brand that reflected the best of our legacy while keeping an eye on our collective future. Having previously led global brand strategies for Kellogg’s and Sony Electronics, I led this project through three distinct stages: discovery, value proposition and design.

Following the nearly four-month discovery phase, where we solicited industry feedback on what ACAMS means to our members, the project shifted to whiteboard debates among management and the core brand team on how to align the findings and key insights with a new brand identity and corporate strategy. Then came the design phase, when everything had to be translated in a way that reflected the association’s re-energized outlook.

Perhaps the most obvious change is the ACAMS logo: a simple but distinct and somewhat bold design that was literally colored by feedback from our members around the world who pointed out the potentially sensitive cultural

Fernando Beozzo Salomao, global director marketing



nuances and local perceptions of visual elements in preliminary designs that might have otherwise gone unnoticed. With the aim of finding a logo that would best represent ACAMS membership across more than 175 countries and jurisdictions, the rebranding team went back to the drawing board to rework its initial drafts.

A less obvious change, though one of arguably more importance, is a rethink of what ACAMS represents. When our association was first launched in 2001, the world was a different place. In the wake of the September 11 attacks, “compliance” often served as shorthand for anti-money laundering (AML) and counter-terrorist financing, and so the organization began as the Association of Certified Anti-Money Laundering Specialists.

Since those early days, compliance expectations have broadened, and not just for banks and other traditional financial institutions. Today, businesses ranging from digital banks to cryptocurrency exchanges to real estate agencies must implement AML compliance policies and procedures designed to detect and report illicit financial activity. At the same time, the scope of financial crime has grown as well, with new efforts to clamp down on illegal wildlife trade, human trafficking and modern-day slavery, domestic terrorism and other criminal activity that was once outside the purview of compliance.

In light of these changes, the rebranding also signals our broader efforts in the anti-financial crime space with a simplified but familiar name that represents more than AML compliance: ACAMS. Just like International Business Machines with IBM and United Parcel Service with UPS before it, we have embraced the simple and succinct.

However, the rebranding is not only about aesthetics and name recognition. A fundamental part of the project involved deploying localized content to better serve our members around the world as well as enhance how members apply for certifications and take part in online training. Thought-leadership initiatives are also in the works to align with the ACAMS website’s new interface.

The brand’s refresh and enhanced online experience is only the start. The ACAMS product and subject-matter expert (SME) teams are working tirelessly to introduce new training opportunities for members and partners tasked with preventing new methods in financial crime. The ACAMS events team is reshaping how the financial crime prevention community comes together in a time of unprecedented challenges and travel restrictions. Behind it all, the ACAMS marketing team is helping members make the best use of our resources, whether they are attending a virtual conference, studying for a certification or accessing content created by our network of SMEs.

Everyone thinks of changing the world, but no one can do it alone. The changes at ACAMS are not the work of a handful of people who have never met a financial crime compliance officer. They are the outcome of listening to the community at large and representing the passionate individuals who are doing their part to end financial crime and make the world a better place.

Fernando Beozzo Salomao, global director marketing, ACAMS

Unexplained wealth orders–

Looking beyond the headlines

In June 2020, ACAMS partnered with Eversheds Sutherland and published a white paper titled "Unexplained Wealth Orders–Looking beyond the headlines." This article is an excerpt of the white paper. The full white paper with sources and methodology can be found in the footnotes below.[1]

In terms of publicity and the deterrent effect against corruption, UWOs can be considered effective in the U.K.

Even before they became available in the United Kingdom (U.K.), unexplained wealth orders (UWOs) were receiving considerable publicity. UWOs empower U.K. law enforcement authorities to compel suspected criminals and politically exposed persons (PEPs) based outside the European Economic Area (EEA) to reveal their source of funds for acquiring domestic properties and other assets in the U.K. (or anywhere in the world) with a value of more than 50,000 pounds ($65,476). Individuals who subsequently fail to demonstrate that their funds are derived from legitimate sources risk having their assets permanently seized in separate proceedings.

UWOs—which place the burden on the respondent to demonstrate the legitimacy of the funds used to acquire an asset—have been available in the U.K. since January 2018. However, to date, they have only been used in a handful of cases in which the National Crime Agency (NCA) has attempted to seize high-end London real estate from overseas PEPs. In theory, UWOs enhance the powers of U.K. authorities to seize the proceeds of crime where they are connected to PEPs or serious crime.

Reverse burden of proof

There is a school of thought that the concept underpinning UWOs enables the U.K. authorities to side-step the key tenet of English law of "innocent until proven guilty." While the ultimate action leads to in rem proceedings, is it fair that investigative tools, such as UWOs, place the burden of proof on individuals? Legal professionals considered that rather than strictly reversing the burden of proof, UWOs create a rebuttal presumption. According to *Lawyer Monthly*,[2] it is noted that this is not, however, a one-way street in favor of the prosecution. The authorities do still need to establish that:

- The subject of the UWO is a PEP or closely connected to a PEP from outside the EEA
- There are reasonable grounds to suspect that they are involved in serious crime
- There are reasonable grounds to suspect that the respondent's lawful income is insufficient to procure the relevant asset
- There is reasonable cause to believe they have an interest in the relevant asset

By way of example, the court will look at the respondent's sources of income, which are "reasonably ascertainable from available information at the time of making the application for the order."[3] One answer to this challenge is for authorities to establish that there are reasonable grounds to suspect a respondent's involvement in serious crime, or that the respondent's lawful income was insufficient to procure the relevant asset and that there is cause to believe the respondent has an interest in the relevant asset.

The issue of burden of proof is perhaps more relevant to asset freezing orders (AFOs), which can be obtained by a police officer, often without notice, by satisfying a magistrate that there are reasonable grounds to suspect that money has been obtained through unlawful conduct or is intended for use in unlawful conduct. Whereas UWOs have been used on a relatively small scale, AFOs have been much more widely used, albeit with less publicity and generally in relation to considerably smaller assets.

Effectiveness

In terms of publicity and the deterrent effect against corruption, UWOs can be considered effective in the U.K. (even if their usage has been low to date). For example, they have caused PEPs from Nigeria to register their tax affairs while preparing to invest in the U.K. In terms of asset recovery, AFOs that often result from defense against money laundering suspicious activity reports (DAML SARs) independently of UWOs have proven to be much more effective. There is a view that UWOs may not be as effective as Parliament intended in terms of asset denial. Even if the assets are recovered in the U.K., given the high net worth of typical respondents to UWOs, corrupt activities could continue in other jurisdictions and the forfeited assets might be written off rather than risk disclosing other assets to prove the legitimate source of funds subject to the UWO in the U.K. This suggests that a more global concerted effort is needed to secure illicit assets and repatriate them.

The U.K.'s approach, which is focused on a small set of assets within its reach, may well be limited in its effectiveness. However, it is strongly argued that if the U.K. takes action and is seen doing so, it increases pressure on others and highlights their inaction. If the U.K. shows leadership, it can bring pressure to bear in forums such as the G-20 Anti-Corruption Working Group to prod them to do more to combat corruption and the flow of illicit funds. As recommended by the Financial Action Task Force (FATF),[4] sharing the proceeds of UWOs targeting non-EEA PEPs with home jurisdictions could promote further cooperation across jurisdictions. While illicit wealth can be spread around the globe, banks and several professional services are global in nature too. If money flows to branches of a global bank, it represents significant reputational and money laundering risk for the bank involved. The risk is further enhanced if a UWO has been obtained against assets owned by an individual who is that bank's customer or the ultimate beneficial owner of its customer. From a legal perspective, more time is required to assess UWOs effectiveness as the legislation is still being tested through the courts. There is no doubt that UWOs have raised the game in terms of the U.K. being serious about tackling corruption.

Outside the U.K., Ireland's implementation of UWOs (called Proceeds of Crime Act orders or POCA orders) has been effective and acts as a good use case for adoption. The impact of UWOs on the U.K.'s asset recovery cannot yet be measured due to the small number of actual UWOs cases and the ongoing nature of the operations. See Figure 1.

Impact for financial institutions

To date, the impact of UWOs on financial institutions (FIs) appears to be limited largely because there have been few UWOs issued since their inception. As long as FIs are fulfilling their due diligence requirements, documenting their results and reviewing client circumstances regularly, they will have complied with many of their anti-money laundering/counter-terrorist financing (AML/CTF) obligations.

FIs are likely to follow a business-as-usual approach on receipt of smaller-scale independent AFOs—similar to their handling of any court order—with procedures in place to deal with collating information, obtaining authorization and sharing information in a timely manner, including reviewing the risk rating of the client. In contrast, UWOs are likely to need specialist bespoke intervention through escalation to senior managers and legal advisors. A longer-term question for FIs exists in relation to risk appetite. The industry, law enforcement and regulatory supervisors do not want to see de-risking, especially as it applies to foreign PEPs in the U.K. because of a potential for de-risking of U.K. PEPs banked abroad. Any changes to FIs' risk appetite in general remain unlikely as the current usage of UWOs is limited. For FIs, there is no better way to prepare for the receipt of a UWO or an unrelated AFO than having robust business-as-usual controls in place, particularly customer due diligence and enhanced due diligence measures.

Resourcing law enforcement with well-trained staff supported by effective investment in technology is essential in the fight against financial crime

Thorough due diligence at onboarding is essential for long-term lending products with PEPs, as exiting these relationships is very challenging. Money laundering risks, in addition to credit risks for lending products, need to be taken very seriously upfront. If the FI finds itself in circumstances where mortgage or long-term credit holders' activities are considered suspicious, consideration must be given to whether funds used to pay interest and principal payments are the proceeds of crime. If suspicion is established, a suspicious activity report will need to be submitted to the FIU. Since long-term finance products make it very hard to exit a relationship completely, decisions will need to be taken about an exit strategy and how to mitigate money laundering risks.

Essentially, the FI has three options:

- Review whether there are suspicions about the source of funds and, if so, seek a DAML SAR to continue to receive funds and maintain the relationship
- Enforce the charge based on the Interim Freezing Order (IFO)
- Write off the debt

The second option will depend on whether this is permissible under the terms of the IFO. Writing off the debt is unlikely to be commercially palatable depending on value of a loan (typically many millions in the context of previous UWOs) and bearing in mind the difficulty of assigning the mortgage in the market in the light of adverse media.

In addition, complex corporate structures involving multiple opaque layers need to be examined by FIs to confirm that there is a justifiable need for these structures, especially if companies are set up in less transparent jurisdictions. Getting the basics right is crucial.

Next steps for governments, law enforcement and supervisors

For governments, further consideration needs to be given to resourcing the NCA and law enforcement. According to a 2019 Transparency International report, "Although the exact scale of dirty money entering the U.K. is difficult to quantify, the National Crime Agency estimates over 100 billion pounds ($132 billion) in illicit funds impacts on our economy each year."[5] The U.K. National Audit Office (NAO) estimated that only 26 pence ($0.34) out of every 100 pounds ($132) laundered is confiscated from organized criminals.[6] This is a poor record given the efforts from law enforcement.

Resourcing law enforcement with well-trained staff supported by effective investment in technology is essential in the fight against financial crime. The nature of financial crime is such that it needs a law enforcement budget with resources comprised of analysts,

Figure 1:

UWO Cases in the U.K.

February 2018 to February 2020: Zamira Hajiyeva

July 2019: Donna Grew ("serious crime" UWO)

February 2020: Mansoor Mahmood Hussain ("serious crime" UWO)

May 2019 to June 2020: The Baker Case

Zamira Hajiyeva: The NCA secured UWOs in 2018 in respect of two properties with a combined value in excess of 22 million pounds ($29 million), which are believed to belong to Zamira Hajiyeva and Jahangir Hajiyev. Zamira Hajiyeva, whose husband ran a state bank and is in prison in Azerbaijan for fraud, spent 16 million pounds ($21 million) at Harrods. The orders have frozen a Knightsbridge house and a golf course in Berkshire owned by Zamira Hajiyeva. The high court and the appeal court upheld the UWOs. She wants to challenge the orders in the Supreme Court.

Donna Grew: In July 2019, the NCA secured an UWO against a Northern Irish national who lives in London. Donna Grew is suspected of association with serious organized crime including paramilitary activity and cigarette smuggling.[1] The order was part of the NCA investigation into six properties she owned worth approximately 3.2 million pounds ($4.3 million) in total. Four properties are located in London and two are in Northern Ireland. Investigations into her purchases of the properties are continuing.

Mansoor Hussain: The first domestic suspect to be targeted with a U.K. UWO is Mansoor Mahmood Hussain, a 39-year-old businessman in Leeds with alleged deep ties to organized crime in northern England. Hussain is allegedly a "professional enabler" who laundered funds for organized criminals, gave them accommodation and even covered school tuition for the son of a convicted murderer and drug trafficker. Hussain was not known as the target until January 2020, when the NCA obtained a court order to freeze 1.1 million pounds ($1.5 million) in a bank account he controlled through his company, 500 M Limited. The high court ruled last year that the orders were "appropriate and proportionate."

Dariga Nazarbayeva and Nurali Aliyev, also known as the Baker Case: In May 2019, the NCA obtained a series of UWOs and associated interim freezing orders after satisfying a high court judge that a number of properties in London had been obtained as means of money laundering. Several individuals and firms involved in the purchase of the properties, or registered as their owners, were made subject to UWOs, and a large high street bank, Barclays, has been linked with providing the mortgage. The NCA suspected that all the properties in London had been bought with riches embezzled by a notorious Kazakh criminal, Rakhat Aliyev, who died in February 2015. The high court discharged the orders, saying the agency's investigation was flawed and inadequate. The appeal court has refused to hear an appeal. In addition, in July 2020, the NCA faced a legal bill of 1.5 million pounds ($2 million), with 500,000 ($659,287) to be paid immediately.

[1] "NCA Secures Unexplained Wealth Order against Properties Owned by a Northern Irish Woman," *NCA*, July 31, 2019, https://www.nationalcrimeagency.gov.uk/news/nca-secures-unexplained-wealth-order-against-properties-owned-by-a-northern-irish-woman

data scientists and economic crime experts.[7] With respect to encouraging cooperation from other jurisdictions, agreements to share assets confiscated with cooperating jurisdictions will provide further incentive. Providing FIs with a safe harbor and encouraging information sharing between FIs, similar to provision 314(b) of the USA PATRIOT Act, will also increase the speed and efficacy of fighting financial crime.

For law enforcement, supervisors and regulators, small improvements in the ecosystem can make a big difference. There is a perceived tension between FIs and the regulators where the FIs do not feel their good work with the NCA and the National Economic Crime Centre (NECC) receives enough credit in regulatory examinations by the Financial Conduct Authority (FCA). In fact, assisting the NCA and NECC sometimes provides the FCA with specific information to scrutinize FIs further. This tension could be eased by establishing and strengthening the channels between the NCA, NECC and the FCA and crediting FIs where they have played a role in uncovering financial crime. There is a risk that clients may complain to the Financial Ombudsman Service (FOS), which creates another source of tension for FIs to navigate. Best practice guidance from regulators on dealing with FOS complaints would be a welcome move.

Another aspect to consider is supervision of sectors beyond traditional FIs. The depth and breadth of supervision provided to FIs needs to extend to other regulated sectors such as law firms, accountancy firms, high-value dealers and estate agents. Supervisors should be able to rely on these regulated sectors to play their part in achieving regulatory standards like FIs. Increased focus on supervising designated nonfinancial businesses and professions (DNFBPs) will increase transparency and deter money laundering further.

Conclusion

While UWOs are certainly powerful tools for fighting financial crime, effectiveness of the regime will also depend on the overall transparency within the ecosystem. FIs have carried the main burden of AML/CTF measures to date. The focus on FIs can be considered right given the number and volume of transactions they process. Regulatory supervisors must pay more attention to DNFBPs. Law firms, accountancy firms, high-value dealers and real estate firms would benefit from enhanced scrutiny by their respective supervisors in the way that they fulfill their obligations. In fact, it seems that supervision of DNFBPs needs attention globally. Consider Australia, where "tranche 2" of anti-money laundering (AML) reform is still awaited after being in the works for over a decade; or the U.S., where lawyers continue to operate in an unregulated environment with regard to AML. Increasing transparency across all industries will make it much harder for bad actors to conceal the proceeds of crime. In an ecosystem of increased transparency coupled with an effective supervisory regime, UWOs can be a powerful tool to fight financial crime.

Shilpa Arora, CAMS, AML director - Europe, Middle East and Africa, ACAMS

[1] Shilpa Arora and Steve Smith, "Unexplained Wealth Orders—Looking beyond the Headlines," *ACAMS and Eversheds Sutherland*, http://files.acams.org/pdfs/2020/UWO-White-Paper.pdf

[2] Dominic Bulfin, "Unexplained Wealth Orders: Guilty until Proven Innocent?" *Lawyer Monthly*, October 8, 2019, https://www.lawyer-monthly.com/2019/10/unexplained-wealth-orders-guilty-until-proven-innocent/

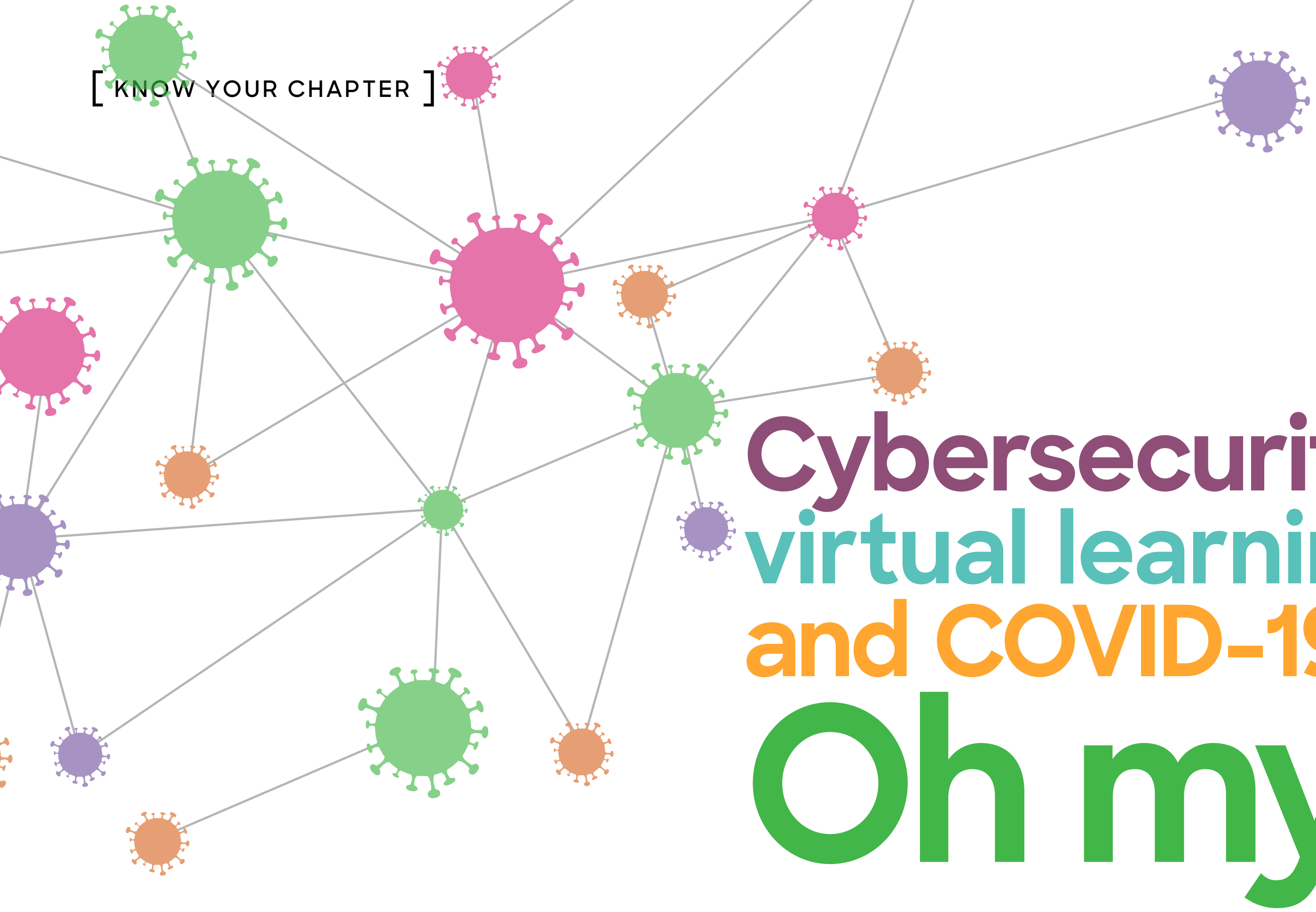
[3] "Criminal Finances Act 2017," *legislation.gov.uk*, 2017, http://www.legislation.gov.uk/ukpga/2017/22/part/1/chapter/1/crossheading/unexplained-wealth-orders-england-and-wales-and-northern-ireland/enacted. See Section 326b Subsection 6 (d).

[4] "Best Practices on Confiscation (recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery," *Financial Action Task Force*, October 2012, https://www.fatfgafi.org/publications/fatfrecommendations/documents/bestpracticesonconfiscationrecommendations4and38andaframeworkforongoingworkonassetrecovery.html

[5] "At Your Service: Investigating how UK businesses and institutions help corrupt individuals and regimes launder their money and reputations," *Transparency International UK*, October 24, 2019, https://www.transparency.org.uk/publications/at-your-service/

[6] "Confiscation orders," *National Audit Office*, December 17, 2013, https://www.nao.org.uk/wp-content/uploads/2013/12/10318-001-Confiscation-Book.pdf

[7] "Call for Financial Crimes Detectives to Be Included in Police Recruitment Drive," *Express & Star*, January 25, 2020, https://www.expressandstar.com/news/uk-news/2020/01/25/call-for-financial-crimes-detectives-to-be-included-in-police-recruitment-drive/



Cybersecurity, virtual learning and COVID-19— Oh my!

The ACAMS Greater Twin Cities Chapter hosted the first of a two-part virtual event series exploring cybersecurity on Thursday, June 18, 2020. What was originally scheduled to be an in-person cybersecurity summit and spring learning event evolved as COVID-19 took hold of the Twin Cities. Interestingly, while the board are experts in their fields, they had plenty to learn when it came to hosting a virtual learning event. Luckily, the guest speaker was a pro!

Mark Lanterman, chief technology officer of Computer Forensic Services, held a presentation titled "Easiest Catch: Don't Be Another Fish in the Dark 'Net'"—a sneak peek into his 28 years of security and forensic experience, which was spent in both the public and private sectors. He also included recommendations around avoiding cyberthreats and improving cybersecurity. While extremely informative, it was Lanterman's storytelling that captivated the audience and made for a thoroughly enjoyable virtual experience.

Lanterman told a story about exonerating a professional athlete after the sports figure was framed as an abuser through digital manipulation. The details were in the data, the key piece of evidence hidden on a device. While the individual accused was proven innocent, his reputation was permanently damaged. Reputational risk related to anti-money laundering/counter-terrorist financing is a known risk for any organization, but cybersecurity vulnerabilities can also do long-lasting damage. According to Lanterman, in one of many publications he shared with the audience post-event, "There is very little public forgiveness for victims of cybercrime, especially when it comes to the perception that personal data has been mishandled, stored insecurely, or collected without full disclosure or permission."[1]

Lanterman also shined light on the ease with which a cyberattack can be launched. Bad actors already have access to personal data, which is available for purchase on the dark web due to previous hacks. These bad actors can easily pose as a trusted colleague, company contact or recognized platform (i.e., Outlook support) by sending a malicious email. Through repeated phishing attempts, these experts are simply waiting for users to slip up—either clicking a link or opening an attachment. If users are fooled, they basically hand over their login/password information as well as the key to the castle.

As many people now work from home in response to COVID-19, they use personal devices and log in through virtual private networks, always one wrong click away from opening the door to an entire company network. "It is always important to acknowledge that wherever we gain benefits from technologies, we also lose security. An increased reliance on the Internet of Things, paired with a recent focus on remote work, contributes to the need for increased risk mitigation and security awareness," Lanterman stated. He went on to explain that the bad guys are also quarantined, having all the time in the world to find vulnerabilities and plan cyberattacks.

The following are Lanterman's key takeaways:

1. Everyone is responsible for building a strong security culture; education and training are critical for combating a changing cyber landscape.

2. Proactive and reactive security strategies should take into account the human element of security—avoiding the "set it and forget it" mentality requires support from every department, not just IT.

"Part 2, Cyber Forensics and Hacking"

The Greater Twin Cities Chapter hosted "Part 2, Cyber Forensics and Hacking," on Thursday, July 16, 2020. Kristy Livingston, IT security manager at MoneyGram, and Jake Bernier, red teamer at a Fortune 500 bank, walked the chapter through their roles, as well as how they support and protect their organizations.

Livingston laid the foundation for cybersecurity by walking through framework, process and data. She then went on to discuss the importance of thinking like the criminal element to get into the criminal perspective—"how would YOU commit the crime?" Next, she touched on funding in individual organizations and understanding the ask, highlighting the importance of key performance indicators to leadership. She shared a couple personal stories with essential reminders:

- **Never dismiss charts and maps:** A case that went 2000 miles to catch a predator.
- **Think outside the box:** A case involving photographs and videos, organized by date and time to determine the location of a sexual predator's victims.

Bernier took the chapter deeper into the criminal mindset, explaining how his team uses tactics, techniques and procedures to emulate real-world threats with the goals of training and measuring effectiveness of the people, processes and technology used to defend an environment. He shared real-world examples of email compromise and then took the chapter on a tour of hacking attempts, in near real-time, further strengthening the importance of personal responsibility.

Livingston and Bernier rounded out their presentations with the following best practices:

- Avoid password reuse
- Use multi-factor authentication
- Scrutinize email requests
- Be suspicious of pressure
- Be careful what you post on social media

They also emphasized the importance of working together—breaking down silos across teams and functions, as well as correlating data across teams.

The combined knowledge of these three experts, over two learning events, was extremely interesting and alarming, especially as the chapter members face new and evolving risks associated with the pandemic. Thankfully, everyone walked away with better cybersecurity awareness.

Board key takeaway

For those chapters yet to venture into virtual learning, the ACAMS Greater Twin Cities Chapter highly recommends it.

Lesley Park, CAMS, co-event/speaker, director, ACAMS Greater Twin Cities Chapter, lesley.park@tr.com

[1] Mark Lanterman, "Cyberattacks and the costs of reputational harm," *Bench & Bar of Minnesota*, October 2018.

Jake Bernier, red teamer at a Fortune 500 bank

Mark Lanterman, chief technology officer of Computer Forensic Services

Kristy Livingston, IT security manager at MoneyGram

Justine Walker:

Keeping up with the pace of sanctions

ACAMS *Today* interviewed Justine Walker, ACAMS' head of global sanctions and risk, about her career in anti-financial crime (AFC) and what she enjoys about working at ACAMS. Until December 2019, Walker was the director of sanctions policy at UK Finance. The former chair of the European Banking Federation Sanctions Expert Group, a position she held from 2015 until December 2019, Walker has held specialist policy positions in the United Kingdom (U.K.) at the Financial Services Authority (the predecessor of the Financial Conduct Authority) and the Treasury's counter-terrorist and proliferation financing branch. She has further acted as an International Monetary Fund advisor on the Nigerian anti-money laundering (AML) and counter-terrorist financing capacity-building program. While based in Central Asia with the United Nations (U.N.), she also worked on programs surrounding weapons and drug trafficking, corruption and terrorist financing, and has served as a national expert on financing of weapons of mass destruction matters.

Walker has extensive experience working with foreign governments, international bodies and financial institutions (FIs) on cross-border sanctions matters. This includes acting as an independent expert to the U.N. and other bodies on the promotion of payment channels in support of permissible international humanitarian activity within sanctioned and fragile jurisdictions, particularly Syria. On behalf of the Alliance for Financial Inclusion and under the auspices of the German G20 presidency, she prepared the special report on financial access for forcibly displaced persons.

Within ACAMS, Walker is tasked with leading critical industry and public-sector relationships, including engagement with key international bodies and think tanks. She holds a Ph.D. from the University of St. Andrews and an M.S. from the University of Edinburgh.

ACAMS Today: **What drew you to a career in AFC and sanctions in particular?**

Justine Walker: I was working in a role in Scotland covering drugs misuse and the policy on drugs misuse, including the response from law enforcement, the social response, rehabilitation, working with parents who were drug users, working on support for their children and so on. I was always interested in the international side of the drug trade, so I was very lucky to secure a position on this with the U.N. in central Asia. That role is what really what took me into the financial crime space because when you start to work with drug trafficking issues and the harm on communities and individuals, you start to deal with the finances behind this crime. What does that level of criminality mean for governments, for stability at the state level and for organizations' stability?

When I was working in central Asia, I was dealing with the drug trade across the entirety of trafficking and inception issues, but also looking at the funding from the drug trade and how that was being utilized by all warring parties. My Ph.D. focuses on Central Asia and the interrelationship between drug trafficking and insurgency finances. That led me into the insurgency and counterterrorism sector, looking at the movement of drugs and the related funds, how that money was laundered, and how local corruption and state corruption were impacted. I continued doing that for a number of years, then I returned to the U.K. and started working with the financial regulator on international financial crime issues.

An opportunity then arose to move into a specialist government role where I was tasked with developing counterproliferation and counterterrorism strategies. This led to a national expert role with a European project on counterproliferation financing. During this period, I was part of the U.K. delegation to the Financial Action Task Force (FATF) and contributed to numerous FATF reports. I was also head of the U.K. delegation to the Eurasian Group, a FATF-style regional body. Being head of delegation sounds very grand but at that point I was the only U.K. attendee! That was the road map I followed into financial crime and sanctions.

I have been fortunate to be in the right place at the right time and build that expertise. But I have also really valued the opportunity to look at these issues from different perspectives. I started from a community perspective, looking at the impact of drugs on communities, then I evolved into looking at that at the source level. What does the opium trade mean for communities, local governments, corruption? What is the international dimension and connection with the global financial system? Then there is the whole nexus of fragile states, conflict states, terrorism. I have been very privileged to look at that from a western point of view but also to spend time in countries that are on the ground fighting this and understanding what that really means for those countries. Sometimes, the policy at the international level does not translate the way you think it would or should translate and the impact can be quite different. This holds true whether you are talking about drug trafficking, counterextremism, AML and so forth.

AT: What does a typical workday entail for you and what do you enjoy most about the job so far?

JW: The first thing I always do when I wake up, much to the annoyance of all my family, is look at the news. I am obsessive about looking at what is happening in the world. For my job, you must understand what is happening in the geopolitical risk environment and how that may influence your work over the next few months. So, the job can be quite fluid depending on what we are working with at a particular time.

What I really enjoy about the job is the global nature and the enthusiasm from the community to deal with these issues. I also enjoy working through a lot of the thinking and the challenging issues of sanctions implementation. This includes working across a diverse sector of stakeholders to look at what this means from an implementation point of view and holding dialogue with governments, FIs, corporations and humanitarian actors on how this is being implemented, what it means and identifying the challenges.

Everything with sanctions is so fluid and can change quite dramatically, which I just love. You can never sit back and relax, you can never be complacent, you must really look and try to understand the detail around them and the potential impacts. Quite often sanctions impact in ways no one considered.

The other aspect of the job is being in the global role, looking at the same issue from different parts of the world and managing that global dimension. It is something I appreciate having the opportunity to do.

AT: Could you share the industry and public-sector partnerships you have been leading with ACAMS?

JW: By way of setting up the international taskforce, we have been trying to bring together a key group of cross-industry experts to work on some major thematic issues. For example, a group was set up to begin looking at the work with the maritime industry and what it means for compliance, whether you represent a bank, a flag registry or a commodities trader. The sanctions advisory and expectations around the maritime industry have really grown. Now, we are unpacking the new norm and what implementation will look like across different sectors. That has been a significant piece of work. It has also been fun, bringing in different stakeholders—energy companies, shipping companies, banks—and getting them all at the table. Hearing different stakeholders' views on the same issue and then finding the common ground can be a quite fascinating.

Another aspect that we have been working on has been around the humanitarian space by way of bringing together a whole different set of stakeholders, including the U.N. This has come to the forefront because of COVID-19 and the need to ensure the movement of certain humanitarian goods, like medical equipment, to Iran, Venezuela or Syria. We have also been looking at what that means for longer-term projects.

In June I was honored to present at the U.N. to the Counter-Terrorism Committee Executive Directorate and have the Assistant Secretary General chair that meeting. I presented on the "Risk Management Principles Guide for Sending Humanitarian Funds into Syria and Similar High Risk Jurisdictions," which I published in May with the backing of the European Commission, U.K. Department for International Development, Swiss government and the World Bank. Securing the backing of these organizations, plus bringing together all the stakeholders involved, took many years of collaborative effort. A lot of dedicated individuals have been involved with this journey and it was a highlight for me to present.

More broadly, we are also working on a range of areas around proliferation financing. We have been looking at the next stage of the Royal United Services Institute and ACAMS proliferation financing study and how to make counterproliferation financing controls more effective. Given my background in this area, I often look at the issue through a very operational lens. Many of the issues that we are discussing now are still the same issues from when I was in government but what has significantly changed is the technology and how access to information now is greater than what it was 10 to 15 years ago. How do you manage the new challenges of having access to so much information, what is important in all that information and how do you interpret it?

We are also trying to build up a greater ability for public-private sector dialogue. What are the areas within sanctions programs that are not well understood? What are the areas where it just does not seem that the guidance given on a certain program reflects the intended objectives of that program? We are trying to bring together the public and private stakeholders to look at what is required, what is meant and help those imposing sanctions understand how they are being interpreted on the ground. ACAMS does not take any view on whether individual sanctions regimes are correct or not. What we try to do is educate our members on what these sanctions mean by way of practical implementation.

Beyond that, there is a lot on general control frameworks, whether it is sanctions screening, risk assessment or audit. That is an ongoing piece of work, so there are some individual workstreams and then there are some ongoing pieces of work.

AT: Do you have any tips for our members on how to navigate sanctions in 2020?

JW: My first tip is you must make sure the basics are there. So much of sanctions now is reliant on having the correct due diligence framework in place, knowing what lines of business your customers are in, knowing where they are geographically exposed and understanding how you may be indirectly impacted by sanctions. One of the first steps is making sure the nuts and bolts are there, similar to any other element of financial crime, and that they are working sufficiently. If you do not have good information in your systems, you are often not able to utilize that information to know your exposure. There is an element of making sure your core financial controls are robust enough and of course that is across the board.

> *To anybody with a global footprint, be mindful of how you manage conflict and cross-border sensitivities*

Another aspect is understanding how you are going to keep up with the scale and pace of change. The pace of sanctions now can be so quick, it is so linked to the wider geopolitical situation, you must ensure that you are interpreting that situation and you are looking at where your exposure may be. This depends on the type of institution. For example, if you are a global institution, your exposure will often be downstream or through your customers' business portfolio. Understand where your downstream risk is and how to navigate that. I would also advise ensuring that the core controls are sufficient and that the information you hold is updated. Also, be very clear with how you are going to manage horizon sanctions and changes to sanctions regimes that can be very dramatic.

To anybody with a global footprint, be mindful of how you manage conflict and cross-border sensitivities. You need to be clear that you are managing your regulatory obligations across the world. This is not as straightforward as it was a couple of years ago.

The final element to consider is that up until a couple of years ago, many FIs would just withdraw from a sanctioned environment and wouldn't do business with a sanctioned country or a sanctioned individual. But now the merger between what is and is not permissible is a lot more difficult to navigate. It can be virtually impossible to isolate yourself from major economies with potential sanctions considerations, so you need to have a much more sophisticated framework. What we had five years ago does not reflect what we now require so you need to ensure that your framework and internal controls have evolved with the scale and pace of sanctions changes.

AT: When you are off the clock, what do you like to do in your spare time?

JW: I am an outdoors person—I kayak, I ski and I have a passion for horses.

Interviewed by: Stephanie Trejos, CAMS, associate editor, ACAMS, strejos@acams.org

ADVANCED
CAMS®
FINANCIAL CRIMES
INVESTIGATIONS

ADVANCED
CAMS®
AUDIT

ADVANCED CERTIFICATION GRADUATES:

Graduates countries/regions are sorted alphabetically

Aruba

Henri Rajan, CAMS-Audit

Australia

Irina Samoylova, CAMS-Audit

Canada

Rebecca Ip, CAMS-Audit

Hong Kong

Nga Yee Monica Hofmann, CAMS-Audit

Japan

Yusuke Araki, CAMS-Audit
Ryosuke Hamagashira, CAMS-Audit
Rie Ishikawa, CAMS-Audit
Aya Kishie, CAMS-Audit
Hitoshi Nakao, CAMS-Audit
Masashi Ono, CAMS-Audit
Junichi Takeda, CAMS-Audit

Jordan

Ahmad Jaber, CAMS-Audit

Laos

Sisavad Chanthalangsy, CAMS-Audit

Lithuania

Edvardas Gudaitis, CAMS-Audit
Tomas Kakanauskas, CAMS-Audit
Enrika Masalskiene, CAMS-Audit
Andrius Merkelis, CAMS-Audit
Neringa Mickeviciute, CAMS-Audit
Monika Narbutaite, CAMS-Audit

Netherlands

Shashank Mohta, CAMS-Audit

New Zealand

Stuart Hansen, CAMS-Audit

Puerto Rico

Richard Morris, CAMS-Audit

Qatar

Ahmad Al Najar, CAMS-Audit
Delia Morna, CAMS-Audit

United Kingdom

Jon Harvey, CAMS-Audit

United States

Yukihiro Nakamura, CAMS-Audit
Nate Suppaiah, CAMS-Audit

CAMS
CERTIFIED ANTI-MONEY LAUNDERING SPECIALIST

CAMS GRADUATES:

MAY-JULY

Graduates countries/regions are sorted alphabetically

Afghanistan

Mohammad Asim Faisal

Algeria

Sara Izerouine

Andorra

Eva Padros Ribas

Anguilla

Ojeda Orielle Vanterpool

Antigua and Barbuda

Louisianne C. Josiah

Argentina

Daniela Laura Garfunkel
Nahuel Peña

Armenia

Anush Abazyan
Tatyana Margaryan

Aruba

Mirjam Auwerda-Jansen
Jeanne M. G. Bislik-Oduber
Henri P. Rajan
Sharona Seneca Sapuana

Australia

David Anderson
Armina Antoniou
Grace Xiao Fen Bacon
River Cheung
Maureen Chun
Julie-Anne Coghlan
Caitlin Cook
Keisha De Saram
Bhathiya Ekanayake
Kristina Ellis
Ryan Emirali
Melanie Gration
Stuart Hallows
Todd Harland
Adriana Maree Hendrickson
Kate Hilgendorf
Chien-leng Hsu
Jessie Kovac
Archana Krishnamachari
Srividya Krishnaswami
Glenn Leyden
Yiran Li
Robert Linnett
Cindy Catherine Liong
Kavita Mandhyan
Susan McHeim
Vinayak Mohandas
Tess Moxey
Akhila Murthy
Thien An Nguyen
Ben Payton
Emilija Poposka Kardaleva
Ashok Pothen
Bharath Prasad
Kevin Prendergast
Hilary Randall
Elaine Roberts
Warrick Round
Irina Samoylova
Sakimi Tehanit Samuels
Adam Shaw
Henry Mark A. Solomon
Ni Alice Diem Kiell Tran
Jing Wang
Hin Chion Adrian Wong
Kit Teng Wong
Jingwei Nick Zhou

Austria

Lydia Lukas
Sandra Luksic
Lisa Nagiller
Bernhard Pelzmann
Oxana Reichenbach
Michael Nicholas Schurian
Marina Yosifova

Azerbaijan

Almaz Musayeva
Bora Onvural

Bahamas

Tamika S. Bodie-Dean
Gabrielle E. Campbell
Carl R. Culmer
Michael Halkitis
Lakera A. McSweeney
Ashley Danielle Moree
Cleinard O. Munroe
Tamika Roberts
Aisha Russell
Ava-Nicole O. Smith
Monica Stuart

Bahrain

Nadia Abbas
Mike Chifisi
Husain Ghuloom
Zainab Habib Alhalwachi
Rahul Rawat

Bangladesh

Md Amir Abdullah
Muhammad Maruf Ahmed
Sharmin Akhter
Mohammad S.-Ul Amin
Md. Jakir Hossain
Muhammad Kabir Hossain
Md. Shamim Mia
Mohammad Z. Hasan Molla
Ehita Tahmina Nazir
Mohammad Shamsuzzoha
Md. Nasir Uddin

Barbados

Keita Danielle Haynes
Keisha D. King-Porte
Inga C. Millington
Sophia Nurse
Janelle Marie Skeete
Jenne Theodore

Belgium

Sophie Wen Y Cheung
Lilian Flavia Da Cruz Paiva
Marion Dapogny
Cyprien De Schepper
Lisa Derijcke
Anninka Truyen
Benoît Waltregny
Jing Wu
Brice Xhauflaire

Bermuda

Peter L. Aldrich
Anthony Garzia
Rachael Harrison
Samantha Laws
Gregory J. Rose
Takiyah Burgess Simpson

Botswana

Kgosietsile Tefo Mogende
Mosireletsi M. Mogotlhwane
Chawapiwa Mpatane

Brazil

Giovani Agostini Saavedra
Michelle B. F. de Araújo
Mariana Bacchin Afonso
Guilherme Pavone da Costa
Gabriela da Cunha Rocha
Felipe Gomes L. de Moraes
Nilo Junior De Oliveira
Gad Disi
Felipe Noronha Ferenzini
Diogo Higino do Nascimento
Danilo Junior
Barbara Saturnino Leme
Robson Toshimitsu Ohosaku
Anderson Luiz P. de Paula
Natalie Ribeiro Pletsch
João Marcelo R. Sant'Ana
Daniel Santos
Ronísio Xavier Junior

Bulgaria

Aleksandra Czeterbuk

Cambodia

Wy Hoong Wong

Cameroon

Gaëlle N. Kousok

Canada

Areeb Mohammed Abdulla
Kwame Adomako
Stephen Oyewumi Agboola
Bola Akindoyin
Tazrian Alam
Jeffrey Allen
Ikram Altindag
Ahmed Ammar
Cristina Andreescu
Julian Arcelin
Sayali Aroskar
Tanvir Ashraf
Olayemi Awobayikun

Antara Basak
Envis Begaj
Remzi Bekfilavioglu
Akeem Olumide Bello
Nathalie Benguigui
Stacey Benham
Sheddine K. Bennett
Elyse Bernier
Taleen Maria Boudakian
Terence Boui
Michelle Brophy
Christine Brown
Samir Buch
David Cauchon
Carolina Certad
Andrea Chan
Anne Chan
Andrew Cheng
Jonathan Chu
Seungyeob Chu
Alex Côté
Buddila Shalinda De Silva
Abhishek Desai
Graeme Deuchars
Ritika Mahesh Dhirmalani
Rommel Domingo
Dorian William Dwyer
Onyeka Ekkeh
Xi Fan
Thomas Feray
Marilyn Caldeira Ferrao
Matthew Froh
Matthew Fung
Vincent Galindo-Serna
Sean Gallie
Michelle Gastle
Priyanka Gaur
Emmanuel George
Emily Gomez
Ali Haider
Sarika Harikumar
Sarah Jo Hill
Vivienne Ho
Lily Huang
Zhuoliang Huang
Michael Philip Hung
Sabrina Husain
Syed Farhad Hussain
Hugh Huynh
Phi Huynh
Maya Inuzuka
Rebecca Ip
Sam Ismail
Laura Katrina Elfridia Jacobi
Shahood Javed
Zhenzhong Jiang
Michelle D. Jones
Janice Karry
Amal Kashyap
Manika Kaul
Temitope Kentebe

Tin Oi Louisa Kwan
Diego Lafaiete Courty Leite
Ashleigh Lapointe
Ka Ho Dominic Lee
Kateryna Levchenko
Feng Lin
Sunny Liu
Shirley Ly
Iryna Lytvyn
Nikhil Mahajan
Jatesh Makalinkam
Sandra Makortoff
Harry Mangat
Martin Marcone
Ali McKenzie
Min Meng
Camaro Mero
Marty Misikowetz
Soumitra Mittra
Ralph Naoum
Aliia Nurkanova
Tommy Olayemi
Ayotunde Omosilade
Niamh Maria O'Shea
Claudius O. Otegbade
Vamsi Sai K. Parvataneni
Dennis Pederson
Miroslaw (Mirek) Piecuch
Danilo Simoes Portela
Apurva Prabhudessai
Frank Preziosi
Maheshwaree P. Veeren
Muhammad Manzoor Rab
Mehnaz Rahman
Mohammed Nahid Rahman
Rajeswar Raja
Rajeev Ranjan
Wu Fei (Elizabeth) Ren
Dairo Riano Castillo
Kathlina N. Royal-Preyra
Kristina Rudko
Aryan Sani
Sarah Carreira Santos
Roxana Sereshteh
Merna Sharoubeim
Alexa Shatsky
Teresa Shih
Nejada Sinani
Anil Singh
Kunwar Jeet Singh Kohli
Jie Song
Kripal Soni
Ibrahim Sowan
Sivagini Srirajayogan
Mykyta Stefanyk (Clancy)
Huaian Su
Nisha Sudhakar
Farhana Taskin
Mariana Tataryn
Conrad Tiedeman
Daniel Vacaru

Rana Varatharajan
Mahadeven Veeren
Gowtham Vijayakumar
Praveen Viswanathan
Silva Vranic
Matthew Warne
Ashley Waterfield
Kurt Wedel
Ryan Williams
Alfred Wong
Alexander Woo
Amy Yang
Amy Yau
Beatriz (Carolina) Yepez
Maxim Yusipenko
Betsy Zhang
Janine (Jianing) Zhang
Kayla Nan Zhang
Bingying Zheng

Cayman Islands

Shiona Patrice Berry
Phulmat Christian
Micah Coleman
Borislav Dordic
Patricia Estwick
Stafano Fernandes
Gabriel Hadrich P. Xavier
Gaunett Dave Harvey
Daine K. Hinds
Richard Kerr
Jamie Lawlor
Aeisha P. Lawrence
Susan McKnight
Robert Riley-Gledhill
Ibereayo Shell
Delia Slater
Allyson Speirs

China

Jiawei Ai
Haixia An
Zhuobin Ao
Jingjie Bai
Tiande Bai
Weibin Bao
Xinyue Bao
Cathy Cai
Jing Cai
Lixia Cai
Ningwei Cai
Wanlin Cai
Weigan Cai
Chang Cao
Fengyuan Cao
Qiyang Cao
Wanle Cao
Ying Cao
Xiaorong Chai
Zexing Chai

Zheng Chai
Jiaying Chang
Jingong Chang
Limeng Che
Caiping Chen
Chen Chen
Guojin Chen
Hongwei Chen
Hui Chen
Jia Chen
Jiahui Chen
Jiali Chen
Jian Chen
Jie Chen
Li Chen
Min Chen
Qian Chen
Qingmin Chen
Ranyang Chen
Wei Chen
Wen Chen
Xiaoxiang Chen
Yan Chen
Yingru Chen
Yiwen Chen
Yuan Chen
Yujie Chen
Zhuangzhuang Chen
Zikang Chen
Xiaorui Cheng
Dongfang Chu
Yue Chu
David Dorrien Cooper
Xiaoke Cui
Chen Dai
Jingjing Dai
Yin Dai
Zhibing Dai
Zhubasong Dan
Jinwen Deng
Xiaoxia Deng
Xiaoyuan Di
Yafang Diao
Li Ding
Yi Ding
Yingyue Ding
Jiexun Dong
Lingxi Dong
Mingyue Dong
Xiaofei Dong
Yuangang Dong
Fangfang Du
Shouxin Du
Tianqi Du
Wenjing Du
Bailan Duan
Jiaying Fan
Siyuan Fan
Jiaxin Fang
Yinan Fang
Chunhua Fei

Zhou Fei
Bifeng Feng
Wenbin Feng
Jing Fu
Zhide Fu
Liang Ge
Ping Ge
Liyuan Gong
Qianwen Gu
Shengping Gu
Tingyu Gu
Yulu Gu
Jing Guo
Jingbin Guo
Lixia Guo
Qian Guo
Cong Han
Nana Han
Xin Hao
Jialin He
Qiqi He
Yi He
Yu Hong
Ran Hu
Rong Hu
Xiaobing Hu
Yu Hu
An Sheng Huang
Chaolong Huang
Chenchen Huang
Dan Huang
Hui Huang
Hui Huang
Jingui Huang
Mian Huang
Sixian Huang
Wenjing Huang
Xiaoyong Huang
Ya Nan Huang
Yanbing Huang
Qing Ji
Juan Jia
Yibiao Jia
Hongfei Jiang
Jun Jiang
Liangchao Jiang
Meifang Jiang
Ping Jiang
Rui Jiang
Yijiao Jiang
Zhiyan Jiao
Ji Jin
Shuning Jin
Liumei Jing
Lun Jing
Yaxuan Kang
Xiaolu Kou
Jieying Lai
Yanming Lai
Fang Lei
Lei Lei

Chaonan Li
Chengxi Li
DongLing Li
Fei Li
Guiyuan Li
Hanying Li
Jing Li
Jinghua Li
Jun Li
Kaiyuan Li
Lan Li
Lili Li
Liliping Li
Nan Li
Ruiyin Li
Ting Li
Wei Li
Xiahui Li
Xiao Li
Yan Li
Yang Li
Ying Li
Yiwei Li
Yongjin Li
Yueru Li
Yuqing Li
Zhen Li
Zhenbang Li
Zhengshun Li
Zhi Li
Xiuyun Lian
An Liang
Jing Liang
Yu Liang
Sisi Liao
Xiangrong Liao
Hua-Ping Lin
Linghua Lin
Zhenqian Lin
Can Liu
Chang Liu
Changrong Liu
Haiping Liu
Haixia Liu
Huili Liu
Jiaqi Liu
Jingjing Liu
Jun Liu
Junkai Liu
Mengchun Liu
Mingyan Liu
Qi Liu
Shijun Liu
Shiyu Liu
Tian Liu
Tiefeng Liu
Tong Liu
Wenlong Liu
Xia Liu
Xin Liu
Xuhong Liu

Yan Liu
Yang Liu
Yuan Liu
Zhenyu Liu
Xiaojuan Long
Jian Lou
Binbin Lu
Chunrong Lu
Jing Lu
Yong Lu
Chao Luo
Lingyan Luo
Luming Luo
Min Luo
Rui Luo
Yuyang Luo
Qiuju Lv
Jian Lyu
Jiayin Lyu
Shuling Ma
Caixia Mao
Yichen Mao
Yuwei Mao
Dandan Meng
Hui Meng
Jie Min
Jianjun Mu
Lin Mu
Huaqing Nan
Xinxin Ni
Zhonghua Nie
Yuefang Ning
Matthew O'Dowd
Qiqi Ou
Hongyan Pan
HuaJian Pan
Jiangyuan Pan
Jing Pan
Teng Pan
Xiaofeng Pan
YingYing Pan
Zijie Pan
Aoqi Peng
Feixiang Peng
Jingyi Peng
Tingting Peng
Yalin Peng
Sizhu Pu
Cen Qian
Guoqin Qiao
Fangzhu Qin
Qimeng Qiu
Hang Qu
Qian Ren
Xuewei Ren
Zheng Ruixin
Qing Shan
Peng Shao
Zhenyu Shao
Lili She
Bin Shen

Bing Shen
Li Shen
Ping Shen
Zhengze Sheng
Feng Shi
Jia Shi
Jing Shi
Jing Shi
Wen Shi
Xiaorui Shi
Lihong Song
Wenyi Song
Bo Su
Jia Su
Yingjing Su
Jinxiu Sun
Mengyu Sun
Mingyang Sun
Nanxing Sun
Runsheng Sun
Wangjie Sun
Weijia Sun
Yuting Sun
Liang Tan
Ying Tan
Huihui Tang
Jiao Tang
Wanying Tang
Wen Tang
Siyuan Tao
Anya Wan
Aixi Wang
Canyong Wang
Dong Wang
He Wang
Hui Wang
Jianfei Wang
Jing Wang
Jing Wang
Jingjing Wang
Jinxin Wang
Keqiao Wang
Kuili Wang
Lili Wang
Lu Wang
Lu Wang
Min Wang
Nan Wang
Pei Wang
Qianlin Wang
Rong Wang
Shen Wang
Shengnan Wang
Shuzhen Wang
Tao Wang
Tianxue Wang
Xia Wang
Xianglong Wang
Xiaojing Wang
Xiaoman Wang
Xiulie Wang

Xiyu Wang
Xuemin Wang
Xuetao Wang
Yan Wang
Yaxian Wang
Yi Wang
Yuane Wang
Yuman Wang
YuPei Wang
Zeying Wang
Zhenzhi Wang
Zhigang Wang
Shengyi Wei
Xiaolu Wei
Jingfeng Wen
Haoze Wu
Jing Wu
Mengyuan Wu
Qiuying Wu
Shuaiyu Wu
Sisi Wu
Teng Wu
Xian Wu
Yan Wu
Yuanyuan Wu
Yue Wu
Xiaoyan Xi
Chen Xia
Nan Xia
Xi Xia
Qiang Xiao
Xiang Xiao
Zhiping Xiao
Chen Xie
Yanling Xiong
Fang Xu
Guoqiang Xu
Jingjing Xu
Kun Xu
Min Xu
Shenchen Xu
Wenqiang Xu
Wenwen Xu
Xiting Xu
Xixi Xu
Yihong Xu
Yongchao Xu
Zhan Xu
Jianlong Xue
Xiaoli Xue
Haichun Yan
Kun Yan
Yu Yan
Yuting Yan
Bing Yang
Dan Yang
Hao Yang
Jingyan Yang
Yubo Yang
Hanbiao Yao
Yao Yao

Yihong Yao
Yaqing Ye
Zhiqing Ye
Zuoxiong Ye
Min Yi
Jia Yu
Min Yu
Tianxiang Yu
Wen Yu
Yan Yu
Yijing Yu
You Yu
Yuan Yuan
Yujuan Yuan
Zhongjie Yuan
Wang Yunzhe
Tao Yuting
Hongjie Zhai
Xuezhi Zhan
Boyang Zhang
Chao Zhang
Chaoxia Zhang
Chen Zhang
Cheng Zhang
Dongqiang Zhang
Fan Zhang
Fuying Zhang
Hongli Zhang
Hui Zhang
Huiyun Zhang
Jie Zhang
Jie Zhang
Lihong Zhang
Lihua Zhang
Lunqi Zhang
Mengfei Zhang
Miaomiao Zhang
Mingcheng Zhang
Ruotong Zhang
Sihan Zhang
Tao Zhang
Tingyun Zhang
Weiqi Zhang
Xiaohai Zhang
Xiaoxu Zhang
Xiaoyan Zhang
Xiaoyan Zhang
Xin Zhang
Xinyan Zhang
Yan Zhang
Yan Zhang
Yanfeng Zhang
Yi Zhang
Yichen Zhang
Ying Zhang
Yingtao Zhang
Yinying Zhang
Yiqi Zhang
Yisha Zhang
Yong Zhang
Zitao Zhang

Bo Zhao
Dan Zhao
Danlei Zhao
Qiaoyun Zhao
Xinyuan Zhao
Yan Zhao
Yan Zhao
Yanqing Zhao
Yingjiao Zhen
Lian Zheng
Liangji Zheng
Ming Zheng
Rong Zheng
Tingting Zheng
Xin Zheng
Jingyi Zhong
Qi Zhong
Xinghua Zhong
Yuhang Zhong
Danfeng Zhou
Hang Zhou
Lin Zhou
Mengling Zhou
Tian Zhou
XiaoPing Zhou
Yi Zhou
Yu Zhou
Zhenzhen Zhou
Changsong Zhu
Chenxi Zhu
Hong Zhu
Hui Zhu
Jiayun Zhu
Junjie Zhu
Liyan Zhu
Yan Zhu
Yan Zhu
Yuling Zhu
Qingrong Zou
Yang Zou
Jialu Zu
Jinfeng Zuo
Meng Zuo

Colombia

Juan F. A. Degiovanni
Luisa Camilia C. Galindo

Costa Rica

Nimrod Martin J. Porras

Côte d'Ivoire

Assoh Reine E. Affi Epse Bile
Nina Fadiga
Melong Justin

Curaçao

Ariana Luz de Sousa
Dyesse C. A. Hernandez
Emelie Salomé Zulia

Cyprus

Athena P. Constantinou
Venera Dracheva
Eleonora Frangou
Lazaros G. Ioannou
Melina Mavridou
Charalambos Pittas
Marica Saulite
Georgios Savva

Czech Republic

Radka Babjaková
Kirill Gritsenko
Jakub Mino
Lavinia Elena Udrea

Denmark

Jesper Meisner
Monika Wieczorkowska
Christian Winneche

Dominican Republic

Anthony Luis Melo Soto

Egypt

Enas Mohamed El Kandily
Salma Moustafa Hamouda
Ahmed M. Mohamed Elkholy
Sara Mohamed Rashed

Estonia

Andreza Carter
Artjom Morozov
Riina Vainola

Finland

Hrvoje Azapovic
Piia Kyllönen
Sarah Brynn Lyerly
Kirsi Matikka
Marsa Paaso
Mikko Samuli Puhakka
Maarit Sivula

France

Karima Azek
Jean Banaszkiewicz
Manon Belgrand
Burdina
Laura Anne C. Sabbag
Basile Chevalier
Licia Damiani
Djeneba Diabate
Karim Djedid
Jean-Hughes Helstroffer
Binta Keita
Eva Kondombo
Marion Laurent
Eric Le Lay
Clarisse Lebarbier
Quentin Lesvigne
Bing Li
Tiantian Liu
Barbara Pelini
Camille Roberts
Damien Romestant
Christelle Soullie
Heng Su
Rebecca Tekpor
Lu Wang
Mao Zhang

Georgia

Giorgi Chochia

Germany

Serin Abdelhamid
Claudia Bacon
Thomas Ball
Sema Dikmen
Jens Guse
Manja Hasselbrink
Sebastian Heine
Šimon Hofman
Brulinda Imeraj
Mirko Kirschner
Michael Köhn
Mariya Kostadinova
Tetiana Kucherenko
Andreas Leitner
Lisa Nitzsche
Holger Pauco-Dirscherl
Yanira Rodríguez Rodríguez
David Rubin
Carina Schindler
Matthias Schramm
Paul Spang
Jorge A. Tena Ramirez
Jan-Ole Vietz
Svenja Wiese
Quan Zhou

Ghana

Marcel Akomian
Maud Appiah
Sena Augustine
Kweku Mills
Belinda Sowah

Greece

Panagiotis Chountis
Eleni Kokkinou
Pantelis Maltezos
Paraskevas Panidis
Dimitrios Papakonstantinou
Vasileios Papoutsis
Konstantinos Pouladakis
Charalampos C. Stavrinides
Yannis Vraimakis

Guam

Keiko Gloria Borja

Guernsey

Jonathan Barclay

Guyana

Joann Alexis Bond
Areika Low

Hong Kong

Joseph Chun Him Au
Xiu Yu Bai
Pauline Byrom
Deborah Cassidy
Ching Man Chan
Choiyuk Chan
Chun Yat Chan
Daniel Chan Pang Chan
Florence Yuen Yan Chan
Hiu Ying Chan
Hoi Yue Chan
Hon Yee Ringo Chan
Ka Wai Chan
Nga Mung Chan
Po Fong Chan
Sik Ki Chan
Sin Yan Chan
Tsz San Chan
Wai Keung Chan
Wing Yin Chan
Yat Wai Chan
Yin Siu Chan
Yun Ming Edward Chan
Wan Chau
Hsueh Yu Chen
Chun Hin Cheng
Chun Kei Cheng
Jian Wen Cheng
Shing Yu Cheng
Ka Man Cheuk
Ming Ming Cheung
Veronica Lok Yan Cheung
Wing Han Cheung
Yenlang Chiang
Wa Fung Chong
John Edmond Chu
Yee Man Chui
Renee Chung
Mriganka Das
Chung Yan Fan
Wing Shing Fong
Yuen Ching Fong
Aaron Avaneesh Francis
Hing Sim Fung
Jie Guo
Lei Han
Justin Wylie Hatherly
Alvin Che Hei Ho
Chi Hang Henry Ho
Ping Leung Edward Ho
Pui Ha Ho
Sum Yi Ho
Yuk Yin Ho
Nga Yee Monica Hofmann
Ka Yan Iu
Young Joo Ko
Cho Wan Kwan
Hiu Yi Kynthia Kwan
Chung Chor Ronnie Kwok
Jonathan Justin Kwok
Po Yin Patrick Kwong
Prudence Lachica
Chun Yin Lai
Mei Kwan Lai
Fion Lam Yim Lam
Kit Wah Lam
Lo Ting Lam
Tuen-Chung Lam
Athanasius To Tsun Lau
Crystal Shu Chun Lau
Man Yan Lau
Tung Ki Lau
Wing Leong Lau
Wing Sze Lau
Chi Yung Law
Cheuk Tung Lee
Chun Yin Lee
Ming Fung Stephen Lee
San Lee
Tsz Kwan Lee
Chin Wang Leung
Hei Fung Phoebe Leung
Tim Wai (Jacky) Leung
Cherry Li Cheuk Li
Chung Hei Li
Dingai Li
Ping Hei Li
Shu Li
Sze Nga Jane Li
Tze Shan Li
Guoen Liu
Ka Kit Liu
Pak Kei Liu
Yang Liu
Cheuk Lun Lo
Kin Chun Lo
Ming Chung Lo
Cheuk Wah Lui
Chi Chung Luk
Shaozhe Mo
Ka Man Mok
Nyasha Moyana

On Shun Mui
Yik Wa Mui
Nithin Nath
King Hei Jason Ng
Tsz Ho Ng
Wing Chin Ng
Tien Quoc Ngu
Chun Wing Or
Tik Shan Pak
Siu Chung Pang
Sze Ki Pang
Charlotte Patton
Hoi Yee Poon
Satish Pradhan
Sze Nok Pun
Tao Qiu
Zubair Riaz
Amrit Sahu
Pawan Jagdish Shamdasani
Yuet Ming Bonnie Shiu
Pui Lam Shum
Yat Sing Siu
George Peter Sobek
Lok Wa Sze
Ting Shan Tai
Yukie Takahashi
Fong Chi Tam
Yee Shan Nereus Tam
Tan Tan
King Pong Tang
Siu Fai Tang
Siu Kei Tang
Wai Kit Tang
Wing Yee Tang
Christina Tong
Pui Yan Tong
Mei Seong Tsang
Ming Lai Tsang
Mo Yin Tsang
Cheuk Yee Cheryl Tse
Gaetan Vanistendael
Cheuk Wing Wan
Ching Yin Wong
Chun Lung Wong
Chun Shing Wong
Fai Shun Wong
Hok Kwan Wong
Ka Ki Wong
Ka Wai Wong
Kar Chiu Wong
Kin Cheung Wong
Kwan Lan Nancy Wong
Lok Hin Duncan Wong
Sze Kei Wong
Wai Man Wong
Wing Yee Wong
Yue Wing Wong
Yuen Ming Wong
Hoi Yin Helen Wu
Wai Chin Wu
Ting Xie
Kwok Cheong Yeung
Kwong Yeung
Rita Yeung
Stephanie Cheuk Yue Yim
Wing Shing Yim
Chung Sang Yip
Wilbert Steven Yiu
Winnie Sharon Y Yiu
Sze Lok Iris Yu
Shuk Wa Yuen
Terence Tse Kin Yuen
Danni Zheng

Hungary

Gábor Kecskés
Márton Nemes

India

Akash Adlak
Harshita Agarwal
Anupma Aggarwal
Nilufer Akhter
Ishwarya Annabattuni
Guido Bains
A Balaji
Asma Banu
Kartik Barach
Arunava Basak
Narahari Bhakri
Sai Kumar Bommana
Roshmi Borkakoty
Atish Chauhan
Aswathy M. C. Raveendran
Prahladkumar P.Dave
Aditya Deshpande
S. Dhamodharan
Rocky Dharmaraj
Rohit Dhawan
Rashita Diwan
Aman Dixit
T Mohammed Ejaz
Rana H. A. L. A. A. E. Rewany
Gaurav Gangwal
Mangesh S. Gholap
Shubhajit Ghoshal
Shailesh Babubhai Gohel
Shagun Goyal
Janaki Guddeti
Arpit Kumar Gupta
Shubham Gupta
Devrath Harish
Vidhya Iyer
Tija James
Sunil Jerald
Vedhavyasan K R
S. K. Nagendra
Archana Kalavapalle
Kamalesh K. Kamalanathan
Ajit Ashok Karkannavar
Jaidev Karunakaran
Anurag Khare
Deepa Krishnamani
Rajesh Kumar
Aashish Madaan
Aravinth Manoharan
Sonal Marwaha
Puneet Kumar Mehta
Tanmay Mitra
Dhanesh Udayshankar Nair
Satish Navale
Prakash Parmar
Satyajit Patra
Pankaj Patwari
Veeraraghavan R
Devi M S
Priya Sahu
Siddhi Samant
Rokesh Anand Shetty
Ashutosh Singh
Saurabh Singh
Jagjit Singh Matharoo
Venkat Sandeep Somanchi
Kousalya Soundararajan
Leena Sudhadevi
Sravan P. Tadakamalla
Sanjeev Kumar Thakur
Shiwani Thakur
Y. Thanigaivelmurugan
Limisha V
Yeshasvini V
Renin Mathew Varghese
Sajeesh T Varghese
Vivek Verma
Meena
Pallavi

Indonesia

Ika Meuthiah

Ireland

Christina Bisdra
Michael Blackwell
Christopher Doyle
Danny Finnan
Florimon Giacobi
Sabrina Hamper
Marine Hector
Sara-Kate Jordan
Neil McAuley
Edmund McDonnell
Andrea Mesiano
Diane Sands Mooney
Stephen Morrissey
Giovanna Nahhat
Lee Rafferty

Israel

Samantha L. Morgan

Italy

Armando Astorga Jr.
Alberto De Ventura
Xiang Huang
Stanislava Marjanovic
Veronica Ortalda
Vancho Sarafov
Lucia Sorace
Mateja Zorč

Jamaica

Kimone Allen
Rohan Bailey
Tahailia Nickeshia Hudson
Carolyn Dolton Jackson
Charmaine Lewis-Robe
Janelle Muschette Leiba
Lauren Riley
Michael Anthony Robinson
Peta-Gay Alethia Rodney
Cindie Lesley-Claire Russell
Kacia Scott
Antonia Smith
Kelly-Ann Whittingham

Japan

Takayasu Adachi
Miyu Ando
Yusuke Araki
Ayako Fujii
Shiho Fujiwara
Yumino Hamada
Ai Hidano
Tomokazu Hirano
Kaita Igarashi
Kenichi Ikushima
Akiko Inoue
Kenji Inoue
Yoko Ishihara
Hisakazu Ishii
Rie Ishikawa
Yuta Ishikuri
Hiroki Izumikawa
Hidetaka Jonouchi
Koji Kashima
Takahiro Kato
Munseob Kim
Aya Kishie
Atsushi Maehiro
Kazuhiro Manabe
Makoto Matsunaga
Hiroaki Matsuoka
Yuji Matsuura
Kaori Minamoto
Shuhei Miyazawa
Takeshi Mizuguchi
Yudai Mori
Kota Morimoto
Hitoshi Nakao
Haruo Ogawa
Tomohiro Okabe
Shinichi Okada
Yosuke Okayasu
Toru Okuzawa
Misako Sakai
Rina Shield
Kadoda Shigeko
Hiroyuki Shimizu
Haruya Shinozaki
Mahito Shirai
Tomohiro Sugano
Kensuke Suzuki
Tetsuro Suzuki
Hiromasa Takahashi
Yunting Tan
Rena Tanaka
Masahiro Tanio
Mitsuharu Tasaka
Yoko Tsuji (Miura)
Takuya Tsujii
Kotaro Tsuruta
Yurie Yamagishi
Kazuyo Yamanaka
Masafumi Yanagi
Seto Yoshio

Jordan

Esra'a Al Momani
Ahmad Aref AL-Dweikat
Mohaned Zaki Hamdan
Ahmad Omar Ahmad Jaber
Ahmad Tarteer

Kazakhstan

Lingxi Huang
Arif Hussain
Muhammad Rafiq

Kenya

Mbuvi Boniface
Nidaa Darr
Francis Kimwea Kariuki
Ben Kebongo Arama
Wycliffe Atieli Lugonzo
Hawas Garba Matta
Rose Wamaitha Mumbi
Diana Muthoni Ngángá
Brenda Simba
Esther Kambe Wachenje

Laos

Sisavad Chanthalangsy

Latvia

Ilze Akmentina
Vladlena Baranova
Marta Bergmane
Mihails Birzgals

Irina Bolbate
Viktoriia Boss
Marta Cera
Laima Eglīte
Anastasija Jacina
Viola Kalnina
Kirils Kondratovs
Ilze Lapsiņa
Igors Likovers
Evita Ločmele
Vladislava Lohmanova
Karīna Lukaševiča
Ivans Marjasovs
Elena Martinova
Evija Novicane
Maksims Rizikovs
Ksenija Scerbakova
Jevgēnijs Smirnovs
Sigita Steina
Arturs Stimbans
Natalija Terjajeva
Jelena Upeniece
Anastasiia Vasylieva
Janis Vilcans
Kristaps Ziedins

Lesotho

Tiisetso Michael Mokete

Lithuania

Simas Aleksandravicius
Justina Anusauskaite
Laurynas Bagdonas
Zivile Beleviciene
Akvile Bumblyte
Roberta Drakšiene
Edvardas Gudaitis
Giedrė Gurskytė
Odeta Jakaviciute
Tomas Kakanauskas
Indre Kaluine
Asta Kazukauskaite
Simona Kišūnaitė
Ines Kring
Aistė Lubaitė
Enrika Masalskiené
Andrius Merkelis
Neringa Mickeviciute
Kristina Mockute
Monika Narbutaite
Silvija Nemaniūtė
Ieva Paskeviciene
Gabija Ribakova
Kristina Sakalyte
Justina Savicka
Gabrielė Šetkutė
Neda Sirtautaite
Paulius Šneideraitis
Greta Stankeviciute
Agnius Stanulis
Simona Survilaite
Ruta Zinkeviciute

Luxembourg

Marta Arias Muñoz
Fadwa Ben Yahia
Carlo Biondi
Gabriele Caruso
Matteo Cordioli
María Díez-Polanco
Mario Grassi
Niels Hernandez
Charles Humbert
Liselotte Laborde-Castérot
Svitlana Nor
Samuel Parmentier
Apostolos Pistolas
Teodora Popa
Gerald Ralph Taylor
Rachel Tchaptchet
Christine Tchen
Emilie Vande Cappelle
Bei Wang
Wenhao Zhao
Hongnan Zhou

Macau

Chou Seng Chan
Chengxin Chi
Sammy Man Kit Chiang
Man Nga Ko
Weng In Kuong
Chi Meng Lao
Wai Man Phoebe Lee
Jing Liu
Kit Ieng Ng
Xueping Wang
Chi Ian Wong
Iok Seng Wong
Rong Zhang
Yuanyuan Zhao
Zhiwei Zheng
Xin Hong Zou

Malawi

Salome Kapeni

Malaysia

Shahratul Izdihar A. Zaki
Kian Guan Ang
Mohamad I. Bin Jis Safri
Sahiriyamala Binti Farouk
Toon Yin Foo
Prasad P. Ghosalkar
Amit Kumar
Lieu Yien Lai
Manish Malik
Soo Wen Ng
Verghese Panackel Peter
Dineshwri Raman
Suthithra Ramasami
Sujay Seel
Cuiqing Voon
Yee Wen Yap

Malta

Charlon Abela
Ruth Agius
Christine Aquilina
Lesley Ann Baldacchino
Rebekah Barthet
Oksana Bonnici
Clara Borg Bonaci
Franklin Cachia
Elena-Andreea Capatina
Neville Carabott
Liza Marie Cassar
Kimberley Katherine Clews
Kadir Serkan Gurbuzoglu
Laura Herbin
David Lorenzo Álvarez
Darren Mascena
Elise Ann Mifsud
Jonathan Phyall
Yanika Pisani
Monica Sultana
Elena Tabone
Alicia Vella

Mauritius

Nelvyn Todishen Cuttaree
Madvi Jeebun
Khusboo Kumaree Puryag
Smita T.-Bundhun

Mexico

Norma Dely Ayala Carrillo
Jose Alberto B. Tecualtl
Cesar Dominguez
Nayra Sanicte F. Sales
Everardo García Menéndez
Alfonso Eduardo H. Alvarez
Rene Lopez Sanchez
César Manrique Soriano
Ricardo Mayo Torres
Lizbeth Pérez Ramos
Tania Itzel Rosas Gonzalez
Orlando Suárez López
Carlos Filiberto V. Ayala
Martha Veloz López
Rodrigo Yoma Duarte

Moldova

Vladislav Castravet

Monaco

Lilia Boughazi

Morocco

Hecham Alilou

Netherlands

Inna Akopdzhanova
Omar Al-Awa
Ulrike Bakker
Ignacio David B. Cervantes
Adelina Bîrsan
Ibrahim Çalışkan
Aikaterini E. Chatziioannou
Naomie W. Deets
Carolina Garcia Caiano
Carmen Goede
Roger Hanna
Abel Hendriks
Hilde Hertgers
Hay Jacobs
Angelien Kalkman
Diederick Alfred Levi
Xiran Ma
Shashank Mohta
John Mooring
Willem Otten
F. de B. L. P. de la Morena
Diana Ramazanova
Riannah Rijnsburger
David Schelhaas
Pepijn Schreurs
Luc Robert Q. S. van Oyen
Slava Stefanova
Anke Stegehuis
Sanel Sunje
A. van de Langemheen
Rik van der Graaf
Marcus Van Gestel
Stephanie R, Elisa van Lier
Tsjangis van Oostrom
Leonie van Rest
Olivier Virette
Micha Vonk
Marisa Walinga
Can Yilmaz

New Zealand

Ashna Achari
Hong Min (Jason) An
Campbell John Burrowes
Sharon Lesley Campbell
Qihong Dai
Luke Daly
Holly Dance
Colin Dixon
Paul Duke
Christopher Gregory
Stuart Hansen
Payal Kapur
Ahmad Khawaja
Soo Chul Kim
Lianne Maude
Cydney Palmer
Helen Phillips-Hill
Teodulo Punzalan
Juyoung Rah
David Rowley
Shreya Salway
Ayesha Tariq
Alice Tregunna
Patric Turnock
Vitya Velayutham
Anna-marie Visser
Charles Wang Qi
George Wong
Fangzheng Wu
Yajun Xiao
Danny Fan Yang
Nuohan Yin
Philip Zhang Zhou

Nigeria

Braimoh Abubakar
Tolulope Samuel Adedokun
Andornimye Elfreda Adie
Abosede Bamidele Agboola
Olayinka Adebayo Aina
Tokunboh Olusoji Aiyedun
Asma'u Jummai Atta
Esther Dennis
Daniel Christian Etang
Christian Eromose Iriase
Harry Oshota Lawal
Chukwuemeka N. Nwaigbo
Charles C. Ochike
Folusho Olajide-Solomon
Chinenye Ihuoma Oluwole
Olagoke Sayeed Salawu
Oyindamola B. Taiwo

Norway

Are Johaug

Oman

Talal Shabir A. Hadi Sajwani

Pakistan

Wamiq Ahmed
Ibrar Ali
Muzzamal Azeem
Inam Hussain
Syed Arij Ali Kazim
Kai Li
Tingting Lu
Usama Mehmood
Muddesra Razzak
Sehrish Taj
Weiming Wang
Xu Yang

Panama

Paolo Bourelly
Zulma Eliana Riveros Trujillo
Paola Romano

Papua New Guinea

Ma. Cecilia Lunar

Paraguay

Emma Maria D. Jara

Peru

Roberto Julio León Pacheco
Lucy María R. Palomino
Cesar F. S. Maldonado
Cesar Silva Ferreira

Philippines

Abraham Ishmael Abital
Diana Pauline Iraola Belo
Roy Comia
Juvianne C. Cruz
Gabriel Joseph S. Gamboa
Maria Ivy B. Lanuevo
Elvira Matugas
E. J. M. Nepomuceno
Ma. Selina P. Valencia

Poland

Iga Andrzejewska
Rafal Bialobrzewski
Magdalena Bielawny
Adam Brzezinski
Suleiman Bushnaq
Marta Chowaniak
Karolina Chwialkiewicz
Emrah Ciloglu
Klaudia Czerwińska
Bartłomiej J. Dzięgelewski
Grażyna Ergül
Bartosz Fudala
Amr Ghatwary
Anna Grabowska
Piotr Jarzyński
Agnieszka Jeziorek
Pawel Karpowiczz
Mateusz Krasnodębski
Konrad Lange
Jakub Madeja
Rafał Majewski
Małgorzata Marciniak
Marta Marczak
Diana Marek
Mariusz Niderla
Anna Paluch
Krzysztof Pietranik
Maciej Pietruszynski
Martyna Pikala
Cyntia Piotrowska
Fajar Prasetya
Davide Salvaneschi
Kamil Santiago
Dawid Sendecki
Zdzisław Skupień
Mariusz Smolarczyk
Andrzej Sobkowicz
Paulina Worobij
Piotr Zeniewski

Portugal

Andreia Sofia Pires Amaro
Vincent Herve

Puerto Rico

Jessica L. Rodríguez Lebrón
Angielisse Solash R. Munet
Alejandro Luis Sanchez
Maria Luisa Vila Garcia

Qatar

Ahmad Al Najar
Delia Ioana Morna
Toms Varghese

Romania

Alina Andreea Culea
Zsuzsánna Deák
Anamaria Duinea
Melania Grunea
Ionela Murzin
Amelia Stoenescu

Russia

Andrew Bayer
Ekaterina B. Minaeva
Tatiana Vasina

Rwanda

Clement Ayabateranya
James Murego

Saint Kitts and Nevis

Diana Claxton-Whittaker

Saint Lucia

Sancha Gervais-Victor
Natalie Jervis
Zaccheus Jules

Saudia Arabia

Amjad Alhumaidi
Suliman Aljabrin
Mishal Saud Aljuleifi
Alya Mohamad Alkharashi
Enas Saud A. Alsubiee
Nouf M. N. Alyogami

Serbia

Vladan Dimitrijevic
Lozana Spasic
Vesna Vlaisavljevic

Seychelles

Lanna Janice T. Jacques
Sophia S. Therese Servina

Sierra Leone

Monday Utomwen

Singapore

Farah Natalya B. A. Jabbar
Mohamed Jaffer S. Alibahas
Ming Quan Wesley Ang
Devina Anggreni Ho
Hidekatsu Aoki
Yi Xiang Aw Yong
Vijay V. Bharadwaj
Subhodip Chakraborty
Kin Wah Amos Chan
Pui Kei Kerrie Chan
Seng Hong Marcellus Chan
Si Hao Chee
Rachel Lew Chee Hwa
Jiasi Rachael Chen
Yek Chuan Chew
Joanne Chia
Jian Xin Jonathan Chien
Srinivas Chiluveru
Wenkai Chin
Xiu Hui Chin
Pearle Jiun Jing Chng
Amarpreet Kaur Chohan
Wensheng Chow
Sin Kuan Chua
Xi Lei Chua
Yuk Chun Chung
Rupanjit Dullat
James Siew Fai Fong
Di Shun Gabriel Foo
Ming Feng Foo
Pei Ting Cheryl Foo
Suet Ning Rebecca Fung
Pei Yi Goh
Wei Koon Goh
Arne Graeber
Suling Gu
Anthony Hall
Wine Myint Mo Hlaing
Xueling Hong
Lei Jiang
Mingrui Jiang
Janell Joseph
Mallory Isabel Joseph
Senthilnathan Kamatchi
Kee Seng Bradley Koh
Vera Lovelle Kai Na Koh
Prabhat Kumar
Lee Jing Lau
Daniel Xin Hui Lee
Feng Jiet Phoenix Lee
Hui Qin Lee
Lu Lu Lee
Winston Song Lin Lee
Yu Yen Lee
Sheng Foong Samson Leo
Xuan Ming Lew
Cheow Yong Leo Lim
Chong Sian Lim
Jing Hui Lim
Kien Hoe Lim
Ren Jie Lim
Yong Da Colin Lim
Stephanie Limantara
Melody Ziyun Lin
Mei Xin Michelle Ling
Chee Foong Loh
An Yu Ally Loke
Ling Yu Valerie Low
Xiang Cui Low
Prema Sanjay Menon
Abdul Ajeez M. Nafil
Hui Ping Madeleine Ng
Qunkai Ng
Ray Wern Ng
Weng Loke Ng
Yan Zhong Jereld Ng
Yong An Freddy Ng
Zhao Ming Ng
Chung Hoon Ngo
Lydiawati Nur A. Binte Amir
Boon Hwee Oh
Pei Ling Ong
Ying Ying Ong
Maria Britto P. Jeyabalan
Priscilla Mei Kitt Phang
Puay Leng Sam
Xiang Yu Seah
Yi Chuan Kaitlyn Seet
Sanya Sekhar
Hong Jian Jeryl Sia
Chin Kiat Frederick Sim
James Spalding
Qiao Ni Tai
Bernard Tan
Cai Ping Sharon Tan
Jia Qi Tan
Jia Yi Tan
Norman Tan
Roxanne Ayemyatmaw Tan
Teresa Shuk Yee Tan
Wei Jian Tan
Xianglong Tan
Yifan Fanny Tan
Jun Jie Teng
Eng Siong Teo
Kah Hao Teo
Zhao Liang Ivan Teo
Lee Li Ting
Kah Khek Toh
Shumei Wang
Jun Wei Wee
Ki Wen Wong
Li Ping Wong
Elizabeth Ann Wong Li Lin
Qinglin James Wu
Nan Xue
Pei Yi Yap
Shi Min Diane Yap
Kai Leng Yeo
Foo Yong Yao
Wei Sheng Shane Yuen
Yi Jie Yuen
Yoke Foong Yuen
Junhao Zhang

Slovenia

Barbara Kračan
Yuri Sidorovich

Somalia

Abdimajid Abdirahman Ali

South Africa

Martha De Jager
Wesley Luke M. Gibbs
Mohammed Khalid Jahed
Leopoldt Jansen van Vuuren
Daleen Kloppers
M. E. B. Likibi-Kaboulou
Cindy-Lee Mareme
Pheto Moabela
Mamodiehi Jeanette Molefe
Lindokuhle Mtyoki
Sviatlana Niakhai
Samantha Paris
Seshantha Pillay
Matthew M. Richardson
Jamie Rowland
Emile Johan Schlechter
Haseena Seedat
Busisiwe Marcia Shange
Hilde Strauss
Bastian Suntken
Ruta Vanagaite
Noel Zeeman

South Korea

Changhyun Ahn
Yunyeong Ahn
InKwan Cho
Sanghyun Chu
Young In Chung

Ji-yeon Han
Yanping Huang
Heetaek Hwang
Sang hyeon Jee
Sung Bin Jhung
Seoyoon Kang
Ami Kim
BoRie Kim
DukYoung Kim
Eunji Kim
Hakje Kim
Hyejin Kim
HyeMin Kim
Jimi Kim
Jinkyu Kim
Joo A Kim
Junhyok Kim
Tae Hyun Kim
Young Woo Kim
Soon Min Kwon
Taekjun Kwon
Dabeen Lee
DongJun Lee
Enoch Lee
Eunyoung Lee
Jonghyung Lee
Sung Hwan Lee
YongJin Lee
Yun Ji Lee
DongHyeock Lim
Song Miae
Eunji Na
Hui Ouyang
Linlin Pan
Boyun Park
Byoung Hun Park
Ji Min Park
Jongseong Park
Jisoo Roh
Jiyoon Seo
Eunkyong Sim
Joo Whoan Son
Sangwoo Son
Yeri Son
Hana Won
Kai Xu
Seongwon Yang
Seung Ju Yang
Jin ho Yoo

Spain

Azucena Acebes
Derek Martin Benjamin
María José C. Caballero
Elena Garcia Gomez
Beatriz Gomez Gonzalez
Carolina Lopesino Romero
Maria del Mar M. Martinez
G. De La C. M. Fernandez
Duffy Anyango Mugeni
Krisztina Oros
Javier Jesus R. Gonzalez
Álvaro Roldán Prieto
Maria Teresa S. Serrano

Sri Lanka

Shavindri Ruwanka Dias
Don C. W. Kannangara

Sweden

Joakim Ljusberg
Julie Mestdagh
Fredrik Nordqvist
Qiuhong Zheng

Switzerland

Joseph Assaf
Adolfo Edoardo Bader
Pierre Ballay
Michaela S. Brunnhofer
Ricardo Carrascosa Fajardo
Fatima Chabane
Maria Isabel Diaz Hernandez
Alain Eloka
Rim Essafi Kolakowski
Matthias Greiller
José Vincent Marti
David Metz
Josselin Montier
Michèl Nyffenegger
Kristal Piñeros Medina
Francesco Rossi
Fabian Sidler
Kseniia Sterliagova
Sandy Toure
Daniel Infante Tuano
Veronika Yartseva

Taiwan

AnRong Cai
Li-Hua Chan
Chia-Ming Chang
Chun-Lun Chang
Nuan-Chen Chang
Shan Yu Chang
Shih-Hsin Chang
Tsai-ho Chang
Yun-Chen Chang
Chao-Jen Chen
Chia-Hsin Chen
Ching-Wen Chen
Chiu-Fei Chen
Jui-Yu Chen
Lung-Jia Chen
Ming-Chuan Chen
Pei-Chuan Chen
Yi-Wen Chen
Yi-Yu Chen
Yi-Yuan Chen
Yong-Xin Chen
Ben-Yi Cheng
Chi-Chen Cheng
Mei-Ling Cheng
Wen Cheng Cheng
Tai-Yu Chiang
Tsui-Lan Chiang
Peng-Yen Ching
Hui-Chi Chne
Yi Chieh Chou
Hong-Mei Chuang
Chien Jung Chung
Ya-Zhu Ding
Su Hai Fan
Chien-I Ho
Yi-Lin Hong
Hung-Ju Hou
Kuo Li Hou
Chia Wen Hsieh
Kun-Tsun Hsu
Mei-Chih Hsu
Yueh-Nu Hsu
Tzu-Fei Hu
Chi-Chen Huang
Chung Wei Huang
Hsun-Yi Huang
Patty Huang
Wan-Ting Huang
Ya-Ling Huang
Yen-Jung Huang
Yi-Hua Huang
Hui-Ju Hung
Wen Yen Juan
Chia-Ching Kao
Tzu-Ching Kao
Yao-Hung Kuo
Wei-Nian Lai
Yen-Ling Lai
Jau-Yun Lee
Kuanyu Lee
Li Wen Lee
Shu-Hui Lee
Tai-Jung Lee
Chun-Hsiu Li
Hsiu-Chun Li
Mei-Shia Li
Siang Yu Li
Chiungfang Liang
Chia-Chia Liao
Ling-Ju Liao
Chun-Wen Lin
Jr-Chang Lin
Min-Yuan Lin
Shan-yu Lin
Ying-Hua Lin
Yu Cyuan Lin
Chun-Hung Liu
Guan Yi Liu
Hung-Chun Liu
Min De Liu
Wu-I Liu
Yi Ling Liu
I-Wen Lu
Su-Chen Lu
Yi-Liang Lyu
Chun-Hsing Miao
Li-Jie Peng
Yu-Chun Su
Yi Shan Sun
Kai-En Tai
Chin-Kuei Tsai
Hui-Ju Tsai
Yu-Hua Tsai
Chia-Ling Tsao
Pei Tsao
Hui-Ling Tseng
Tsun-Ta Tseng
Mei-Chuan Wang
Mei-Yun Wang
Shu-Ying Wang
Yu-Hsin Wang
Wan-Ting Wei
Chia-Yu Wu
Chung Hsin Wu
I Ching Wu
Shao-Chu Wu
Tsai Ling Wu
Ting Syuan Yang
Min-Kai Zhang

Thailand

Kanyarat Boonyapison
Amornphan Ruwattananon
Niti Sirichit
Siyun Wang
Anthicha Wondaw

Togo

Bintou Ouattara

Trinidad and Tobago

Alissa Ali
Karen Burnett
Luke Tristram Hamel-Smith
Sheldon Harricharan
Andrew Lavia
Michelle Majid
Terrence Osmond Pierre
Akeem Rahaman
Farisha Sally Ramdath
Amar Ramlogan
Rishie Rattan
Angelique Tuitt

Tunisia

Fethi Akkari
Dhieb Atoui
Amel Laourine

Turkey

Ömer Bahadır
Selvi Sinem Balantekin
Melik Bağlş Bilici
Oguz Demir
Ufuk Ömer Erdemoğlu
Hediye Ergen
Bilal Ertogrul
Mehmet Onur Günay
Zeliha Isikhan
Sadık Karaçalı
Ecem Karapınar
Irem Korgen
Kübra Şener
Ahmet Kagan Sonmezer
Zehra Tamay Dede

Turks and Caicos Islands

Myrine Remy

Uganda

Edward Amanyire
Nelly Turyasingura Erongot

Ukraine

Yuliya Bened
Artem Hrytsak
Andrii Zalieskyi

United Arab Emirates

Omar Abdalle
Amira Ahmad
Abhay Alexander
Nouf Alshamsi
Uma Anil
Ebrahim Asadi
Laure Aziz
Onkar Ashok Bare
Murray Brown
Kaushik Chandramouli
Sunil Kumar Chellappan
Christos Christou
Miles Corney
Dencil Davis
Muhammad H. Dawood
Srishti Dixit
Jayaprakash Edayillam

Benoit Ferland
Abdelmonem Gabr
Alfred Gachaga
S. Gopalakrishnan
Navin Goyal
Jun Guo
James Hills
Hiu Ying Hung
Ahmed R. I. Mohamed
Shane Jenkinson
Ramatoulie Jobe
Aiza Kashif Chaudhry
Jefna Khalid
Anbuselvan Kumar
Neeraj Kumar
Sheetal Latson
Victor Daniel Malenab
Jayshree Manikere
Bhavin Mehta
Vinay J S Menezes
Shashank Mishra
Caroline Ngigi
Raman Pabreja
Toni Michelle Patol
Vinita Pherwani
Ramya Naga Poojary
Anne-Lise Aurore Pyday
Ahmed M. Radwan
Girish Raipancholia
Rizwan Saleem
Shashwat Sanyal
Tamiour Shahid
Yusuf Akhtar Shaikh
Tomeshwar Singh
Kalyanaram Sivalanka
Eric Ssempebwa
Chris Thomas
Dilip Uluwaru
Samina M. Umrethwala
Rahul Raj Varakott
Boniface Manyara Waitathu
Syed Noman Weqar
Dina Tilahun Yimer
Madina Zaltsman

United Kingdom

Oluwatofunmi Adedoyin
Faiz Alli
Umar Alvi
Vito Armonavicius
Gamze Asir
Angus W.R. Backhouse
Iqbal Singh Badwal
Charles Baillie
Gregory Barnett
Jade Bennett
Rupert Benzecry
Joshua A.G. Best
Ryan Boyd
Weder Casemiro de Souza
Juanjuan Chen
Ross George Curzon
Adebayo Daniels
Edgar John Davies
Jenny De Pretto
Bhavesh Desai
Beatrice Di Liberto
Adam Dickens
Djan Direkoglou
Alexandra Donnelly
Siobhan Egan
Ben Ferguson
Sandra M. Ferreira
Jon Fowler
Dmitri Gorelov
Anna Grabda
Inayat Haleghi
Emma Hanratty
Jon W. Harvey
Charlie Hayward
Jonathan Ho
Branislav Hock
Asad Hussain
Bhavika Joshi
Julija Jurca
Darren James Key
Conor Kingsley
Simon Knight
Raman Kumar
John Martin Kunjumon
Surfraz Lobania
Yidan Luo
Arun Mattu
Tom McAvoy
Henna Mehta
Anton Moiseienko
Michael “M.” Montgomery
Jemima Bondo M. Mbungu
Yukihiro Nakamura
Alicia Navarro Medina
Muazzim Nawaz
Paul Ogun
Adenike Ojo
Ademola Omosanya
Adeboye Adeseye Oni
Nicholas David Ostler
Ian John Palabrica
Maria Perarnau Bayo
Oliver Wolfgang Perry
Santosh Phutane
Slawomir Popielski
Klaudyna Rajchel
Olga Razeva
Ivana Sainovic
Viacheslav Sheremetyev
Timurs Šihalijevs
Gagandeep Singh
Yvonne Marie Siwek
Christopher Swatkins
Julia Tatarenko
Jack S. Thornborough
Derek Turnbull
Christopher John Usher
Sara Vallejo Martinez
Ware Vercamer
Thomas Vincent
David Walker-Sherriffs
Francesca Walmsley
Samantha Wild
Zeynep Yazici
Stephanie Si Long Yuen
Xiawen Zheng

United States

Yvonne Aaronberg
Timothy Aderman
Adenike A. Adesina
Kwabena Adu-Gyamfi
Nandini Agarwal
Shishir Agrawal
Juan Jose Aguirre
Md Shakil Ahmad
Charles R. Aikins
Mahabubul Alam
Carl Alexander
Mirna Alexander
Deanna Elizabeth Alfaro
Crystal A. Alfonso
Shann Lanai Ali
Wafee Ali
Lucy B. Alorgbey
Yvonne Alvarez
Blanca Amezcua
Jing An
Abhinav Anand
Margarita Anda
Christopher Anderson
Jacob Eivind Anderson
Sherri Anderson
Brent Andrews
Sarah J. Anspach
Annie Anthony
Renaldo Javon Antoine
Fabiola Antonio
Michael Appiah-Antoh
Olufemi Aremu
Matthew Arfele
Nelly V. Arias
Michael Charles Armstrong
Christopher Arnold
Joseph Richard Arra
Kwame Asare
Syed Hassan Askary
Jacob Avery
Toyin Ezra Awoniyi
Micheline Azor-Burrell
Fatema Bagam
Brian M. Bagdonas
Hari Rishi Bahadur
Jacob Baker
Sean Baker
Esther Balassiano
Judith Barendse
Janet Barraza
William R. Baxter
Carey G. Been
Virgil Bellini
Kimberly Bello
Jonathan Benovitz
Brandon Lucas Bergeron
Margarita Bernal
Diann Berry
Meaghan Bever
Larry Bianchi
John R. Bibb
Gerald F. Bingeman
Rosemary Bishara
Kevin Black
Jim Blackwell
Ciara Blair
Kelly C. Blake
Breyn L. Blakely
Pamela Norma Blum
Augustina Boakye
Jonathan W. Bobb
Kevin Boix
Jason Bokser
Christine C. Boler
Chris Bolt
Kebra M. Bolyard
Shivangi Borah
Luca Borgoglio
Matthew J. Boris
Adana V. Boyd
Thomas Brempong
Jonathan Phillip Brenner
Victoria G. Breshears
Rodney C. Brewster
Melanie Bright
Terri L. Brooks
Christopher Andrew Brown
Clara Marie Brown
LaDerek Brown
Kelly Browne
Alexander Brundage
Charlie W. Bruno
Matthew Buchanan
Whitney Diana Buey
Andrea E. Buford
Patricia Buitron
Dorothea M. Burke
Margaret Bustos
William Byrne
Brian Caffrey
Miguel Campos
Adam Cappucci
George Caramanna
Greg Carlile
Ron Carny
Guadalupe Maria Carrera
Mercedes H. Castro
Brett Cerussi
Monica Cervantes
Brett Chambers
Jessica Chambers
Kati D. Chandler
Eun-Mi Chang
Yiming Chang
Lisa Chapman
Kuzivakwashe J. Charamba
Faith Ann Chavarin
Chingsheng Chen
Winnie Cheng
Heather Chester
Terrainna S. Chisholm
Gina Choi
Martin T. Chojnacki
Nathan Chomsky-Higgins
Branden Chowen
Connor Christensen
Stephanie Chua
Seung-Hwan Chung
Elizabeth Cleary-Clark
Jasmine Olivia Clements
Kaitlin Clements
Cassandra J. Clingler
Brendan Francis Cochrane
David A. Cohen
Amela Colic
Lina Maria Comas
Jennifer Congi
Lisa Cook
Jack Coombes
Ashley Victoria Cortes
Nicole Costaldo
Joshua Couzens
William Everett Crack
Blake Edward Crenshaw
Daniel Crites
Chantal Cruz
Maria Cusano
Arturo Custodio Jr.
Sergio Custodio Jr.
Kristin Margaret Daly
William Danks
Jacqueline Vetsera Danner
Evan DaSilva
Andrew Davidson
Jennifer Davies
Harold A. Davis

Pennylane De Jesus
Antoine de Villoutreys
Star Del Castillo
Michael J. Delgado
Frank M. Dellapolla
Michael DeNigris
Jacob Denman
Rosemary DePalma
Alanna DePriest
Michael J. Derevjanik
Halle S. Dickey
Nicholas DiEva
Katie M. Digilio
Angela Ding
Dirisala Satish Dirisala
Christopher M. Dohn
Mark Donato
Ashraf Donn
JoAnne Dorange
Emily Dorris
Anne M. Draves
Gary Morris Dreyer
Richard F. Drill
Nicol Duarte
Christopher Dufresne-Yidi
Stuart W. Dunn
Nibedita Dutta
Brian Dwyer
Justin Michael Eddy
Christian R.T. Edge
Sallie Eileen Edwards
Rebecca Emesih C.
Margaret L. Estler
William Fagerstrom
Cassidy M. Yuhei Fahey
Kyle Fan
Rachelle D. Fannin
Shonnell Faustin
Nicole Ferguson
Jennifer Fernandez
Hilina Fetahi
Brian Fischer
Hannah Fitzgerald
Zachary Hill Fitzgerald
Darrin Flaim
Riece Fleming
Cassandra Fong
Christina M. Fontana
Noelle Foor
Daniel W. Forbes
Meredith Fortier
Starline Fortune
Giovanni Jeanet Foster
Landis Fowler
Andreen Alisha Francis
Tonya Frank
Conner Freeman
Keri A. Freiler

Luisana Frias
Dulce Maria Fuentes
Patrick J. G.
Tiffany Gaines
Saniya Galimova
Kimberly Gallo
Michael Galluch
Adam Galton
Karl Gambin
Danelia I. Garcia
Gabriel Garcia
Vicente C. Garcia
Aiyana R. Garland-Tyler
Eileen Garvey
Jerry Garzon
Austin C. Geraghty
Sean Geraghty
Brian Gillie
Anna Louise Goerler
Tarica Golding
Andy S. Gomez
Nicolleta Goncalves
Jessica Gonzalez
Viviana Gonzalez
James R. Goodwin
Piyush Goradia
Alex Grande
Laura Ann Grapstul
Eliezer Green
Iolanta Green
Tamberlyn L. Greene
Matthew J. Greif
Benjamin Grier
Timothy Lawrence Griffin
Tara L. Griffith
Thomas Grom
Michael Groome
Claudia Gross
Edward Grossi
Jesse D. Guerrero
Ronald Guilbeault II
Nishant Kumar Gupta
Andrew Gustus
Victoria G. Gutierrez
Alan Kent Halfenger
Chelsea Hanniford
Natasha J. Hardnett
Andrea Carole Harris
Laura Harrison
Daniel W. Harvey
Maria E. Hatzopoulos
William Thomas Hayes Jr.
Cristina Hazelwood
Morgan Henry
Stefan Herron
Helen Elizabeth Hester
Alexander Heying
Jamie Lynne Hilborn

Elizabeth Hill
Austin Hong
Brandon Hord
Gloria T. Huang
Laura A. Hughes
Thomas Hulihan
Laura Hunt
Alexander R. Hunter
Edward Alan Huntsinger
Olufemi Ijandipe
Faizan Imam
Neel Iyer
James A. Jackson
Sophie Claire Jacobs
Tina Jacobsen
Pierre Jacques
Fatima Jamal
Morvarid Jamalian
Fawn Jamerson
Piotr Jastrzebski
Romella Javillo
Jerome Jenkins
Katherine Anne Jensen
Jason Jimenez
Lisel A. John
Brenton Johnson
Jessica Johnson
Jessica R. Johnson
Matthew Jones
Nona Jones
TiAndra Catherine M. Jones
Jason Garrett Jordan
Shawn Jordan
Shane Jorgensen
Sukhveen Joshi
Yury Kabakov
Cyrus Kaikobad
Kaveri Kaishan
Mehmet Kalyoncu
Sung (Jimmy) Kang
Mindy R. Kaplan
David R. Karasik
Stephen Ray Keebler
Shawn AJ Kelley
Kevin Kelly
Jacob Kennedy
Nina Kerkez
Joseph Keith Kessel
Rachit Khaitan
Jung ah Kim
William Streeter Kinnard
Paul S. Kitchen
Kinya Knight
Kelvin Ko
Justin Angel Koatz
Avril Koblitz
Adam Kocab
Patricia Koch

Ewa Danuta Koguc
Zachary Michael Kohn
Kevin Tung Sun Kong
Sally Koppes
Katharine Kovacek
Keith J. Koval
Laura Krahl
Kris Krasinski
Ashwin Krishnaswamy
Robert Kuptz
Nyarai Kutepa
Christopher F. Kwan
Christine La Rochelle
Bryce Lackey
Anne-Emilie Laforest
Marissa Lahousse
Nadine Lam
Daniel P. Lane
Jonathon Lane
Stephen Laquerre
Amanda Laryea-Walker
Afis Lasisi
Jacqueline Lavelanet
Anand Lavi
Temitope Ibrahim Lawal
Ashley Laws
Patrick W. Leary
Jared Lee
Jun Gyu Lee
Judith A. Lemon
Wyatt Philip Lemons
Russell J. Lessard
Arava Lev
Courtney Lewis
Esther Li
Rui Li
Zachary Lierley
Shannon Linnemann
Yang Liu
Leon Lockhart
Andrea Noelle Lollar
Sophie Lombardo
AJ Lopez
Ivan Alex Lopez
Virginia Lopez Rubio
Bill Louie
Andiana Louis-Jean
Kristin M. Ludwig
Naomi Nkinda Lupemba
Franklin Lurie
Sarah Lynn
Peggy Ma-Baranovskiy
Pedro Paulo Macellaro
Carlos E. Macias
Michael S. MacNaughton
Sandra L. Maharaj
Keenan Mahoney
Jiaqi Mai

Asmita Maithani
Alejandro Malagon
Luis Ramon M. Medina
Munazzah Malik
Daniel Lee Maneethai
Amara Mansoor
Fadi Mansour
Jason R. Marason
Marcie M. Marsh
Tara Matas
Vanitha Mathur
Benjamin Mattern
Ana Laura Maya
Caroline A. Mayrhofer
Peter Mazaran
John D. McArtor
Dean R. McCarthy
Sarah E. McClure
William McGauran
Tracy Nicole McGrew
Matthew James McIntyre
Stephen G. McKenna
Kathryn E. McKenney
Nicholas Mckim
Tychelle D. McLaurin
Mary Amanda McManus
Dan L. McWilliams
Gary N. Mellow
Michelle Mendivil
Thomas Metcalfe
Andrew Meyer
Justin A. Meyers
Joseph F. Mica IV
Sarah Miller
Jeffery Miller Jr.
Jason Millhiser
Andrew Milord
Dana Mirro
Reginal Timothy Mitchell
Suzanne Mitchell
Patrick S. Mitro
John Mondragon
Trina Montano
Christina Montgomery
Antonio Morales
Chris Morgan
Ethan Morgan
Joseph R. Morrison
Michael Morrison
Jada Morrow
Gregory Moscow
Abdul Mouneimne
Rejoice Muwadzuri Moyanah
Dale Andrew Mulhall
Marian Muller
Mary B. Mumper
Zachary Muncrief
Erandy Munoz

Mary W. Muthee
David Nadler
Sunil Nair
Sana Nasralla
Chioma Ndukwe-Uguru
Christina Nelson
David Nelson
Diane Nelson
John M. Nelson
Teresa Nelson-Morgan
Musette Spruill Nesbit
Jennifer Grace Nestrud
Susan Lyn Newby
Tay Nguyen
Zixin Nie
Martta Niemela Desanges
Stephen Nitao
Joshua Noble
Siad Nor
Pam Obermueller
Alyssa O'Brien
Anna Odoi
Tina Oh
Erika Okumura-Andersen
Katherine D. Oleson
Sofia Oliveros Gomez
Giselle N. Olmo
Oyetunde Oloyede
Kimber Olson
Jennifer A. Otufangavalu
Talal Ouazzani Chahdi
Wenjie Ouyang
Javier Esteban Pabe
Danna Padilla
Mathew M. Pakkattil
Peter Panepinto
Fernando Pardo
Andrew Parks
Aimee Parmentier
Aaron M. Passy
Tapana Kumar Patro
James M. Patterson
Bonnie Pau
Sarmistha Paul
Brenda Pavelka
Laura Alexandra Payne
Ramer Pelayo
Jennifer Wilkerson Pelham
Carrie Anne Pels
Brayton J. Peltier
Isabela Pereira Motta
Lauren Elizabeth Permuka
John Pettibone
Brian Pfeiffer
Julie Phillippe
Sean Pilkin
Albi Pina
Todd M. Pinarchick

Lindsay Pinto
Daniel A. Pittack
Ryan Pittman
Samantha Place
Tammy R. Plante
Diana Carolina P. Enriquez
Austin Dean Pollard
Matthew C. Pomeroy
Stephanie Powell
Canip Poyraz
Jeffrey Pratt
Erin K. Preston
Timothy Colin Pride
Edward Pugh
Tatyana V. Pukhova
Samuel Rager
Meghan Rahman
Kurnia Rahmani
Jonathan Michael Rainey
Anna Marie Rakers
Andrea Ramirez Abdala
Natalia Ramos Nigaglioni
Quinn Ramsey
Dimple Rathod
Keith Raymond
Grace Rebling
Zach Reda
Scott Allen Reeves
Evan Theodore Revak
Derek Richmond
Jennifer Lynn Richmond
John Robert Riemer
Kassia Riggs
Shirley H. Riley
William F. Riley
Harvey Rindt
Jorge Rioja
John Luis Ripoli
Sarah Eve Rivera
DeShawn Takee Robbins Jr.
Lawrence Damian Robinson
Carlos Rodriguez
Jennifer Lynn Rodriguez
Mariangel Rodriguez
Michael Rogero
Kimberly Rolle
Jennifer Marie Romero
Danielle Rongisch
Jason Eric Rosen
Nicholas G. Rosenthal
Benjamin Manuntang Ross
Denielle Ross
Tessa Ross
Jon Rossi
Jennifer N. Roth
Aslihan Routledge
Mark A. Ruby
Michael G. Rufino

David Ruggiero
Kevin Rushing
Mikhail Rusnak
James Dunn Russell
Daniel Rust
Melissa Ryken
Aya Sabayon
Ebenezer KP Sabbi
Elizabeth Vanderwilt Safi
Emmanuel Saget
Maria L. Sahlin-Boyd
Ganiyu Alabi Salimon
Catherine Salinas
Benedict A. Salva
James T. Sangirardi
Mohamed Modibo Sankare
John Santana Lopez
Rolando Santos
Mark Saunders
Brian Schleigh
Aspen Patrice Schleser
Kendra L. Schmidl
Edward R. Schmitt
Violeta Segarra
Susan Senterfitt
Terrill P. Seymore-Green
Sue Ellen Shade
Linda F. Shan
Jyotsna Sharma
Philip J. Shaw
Maxwell Shea
Erik Shipley
Heather A. Shore
Brittney Megan Coley Smith
Rachel Smith
Ryan Mattie Smith
Shandalyn Smith
Marla A. Snyder
Jacob Sobiech
Steven Soggin
Brian A. Soja
Candice Solano
Aakriti Soni
Phyl Nora Sotelo
George Thomas Soterakis
Daniel Soto
Courtney E. Sowden
Linda Spencer
Janelle Springer
Amit Srivastav
Warren Stark
Julie M. Stengle
Spenser Dane Stephens
Beth Ann Stevens
Sophie Stimson
Madeline J. Stoeri
Loren Stokes
Jeremy M. Stone

Malissa Strange
Danika M. Streater
Brandon P. Stymiest
Sarah Styslinger
Thiruchenthil Subramaniam
Sheeba Sukumaran
Nate Suppaiah
Andrew Thomas Sustaita
Christene Swartzendruber
Vernon Tanner
Selene Tarng
Jermaine C. Taylor
Sarah N. Taylor
Tokunbo Ivana Tayo
Jess Tejeda
Kate Tenenbaum
Elizabeth Terrell
Joshua Teslicko
Zeb Tharp
Mel P. Thillens
Erica Michelle Thomas
Susan Thomas
Jason D. Thompson
Robert Thompson
Der Thor
John Tomasovich
Nicholas Tomlin
Nataly Torosian
Maria Torquato
Amber Sims Torres
Karen Torres
Lisa Torres
Danielle M. Tothero
Max Totilo
Felipe Tovar
Ivo Trajcevski
Christopher Trayler
Eric Trelz
Amy P. Trent
Shih Ju (Leticia) Tseng
Julie Lynn Ulrich
Douglas G. Urbanek
Christopher Vacanti
Irfan Vaid
Akshay Vaishampayan
Jessybeth Valentin Seda
Andrew Vasquez
Donna Marie Vazquez
Lariannis Vazquez Morales
Revanth Veeramachaneni
Tatiana Velicheti
Waskar Veloz
Michael Vento
Gilad Erik Vered
Rameshwar Verma
Javier Villarreal
Tatyana Villegas
Monica Vinson

Samita Virmani
Iryna Voitenko
Rekia Walker
Zhen Wan
William B. Wang
Adam Warsoff
Erica M. Watson
Andre Webb
Ashley M. Weed
Amy Weiss
Christina L. Weiss
Nicholas Welch
Marcie White
Niki D. White
Jamie Weigh Whobrey
Cara Wick
Evin E. Wick
Matthew Williams
T. Williams-Lightbourne
Taresa R. Willingham
Jonathan Wilson
George Arthur Wilson Jr.
Stephanie Wise
Malgorzata A. Wojtowicz
Angela Wong
Kingman K. Wong
Joanne Woo
Nuo Xu
Ryo Yamaki
Irina Yarovaya Nahle
Andrew Joseph Yeates
Jung Min Yeo
Rick Yost
Benjamin A. Young
John C. Young
Michael Zeiler
Ji Zeng
Shen Zhang
Xiao Jian Zheng
Ina Zyfi

Vietnam

Hung Quang Trinh

Yemen

M. A. Q. A. Alnawah
Kamal Saal Alawi
Amal Aldubaili
Nabil Ali Thabit AL-Fakih
Abdullah M. Ali G. Al-Farzae
Mohammed Almeeri
Madlin A. Alqubaty
Ayad A. Hussein Kassem

CGSS™
CERTIFIED
GLOBAL SANCTIONS
SPECIALIST

CGSS GRADUATES: May-July

Graduates countries/regions are sorted alphabetically

Australia

Julie-Anne Coghlan
Audrey Fitzgerald
Kylie Oliver
Sarah Genevieve Williams

Azerbaijan

Nargiz Abbasova

Bahrain

Muhammad Bilal Akram
Shelly K. Jose

Bangladesh

K.M. Lutfor Rahman

Belgium

Manoj K. Arora
Priscilla de Schaetzen
Damir Stancic
Benoît Waltregny

Canada

Shadab Ahmed
Albina Alimerko
Tiffany Chan
Seungyeob Chu
Faran Fallah
Tracey L. Foulds
Obrad Grkovic
Vu Chinh Kieu
Martin Marcone
Gyoung Ho Min
Iryna Pisetska
Saurabh Seth

China

Ke Fang
Wen Shi
Jinxin Wang
Yan Wang
Huawei Zhang
Qiang Zhang
Gaoqiong Zhao
Mingjie Zhao

Cyprus

Fotini Ph. Patsalidou

Egypt

Dina Farghaly

Finland

Satu Välisalmi

France

Irène Bach
Xin Dai
David Gagaille
Catarina Pedro de Abreu
Magdalena Seignovert

Germany

Veit Bütterlin
Agnes Eva Checinski
Kirsten Ditzinger
Florian M. Haufe
Holger Pauco-Dirscherl
Karin Porstendoerfer

Ghana

Bismark Sakyi

Guyana

Stacy Wilson

Hong Kong

Ka Leung Jacky Chan
Fu Yan Cheung
Kwok Tung Cheung
Ching Tin Fung
Ming Hang Ho
Esme Hodson
Wing Hin Hon
Yan Sang Kam
Hoi Yi Olivia Kwan
Wing Leong Lau
Yik Tai Thomas Lau
Chun Yin Lee
Joshua Sze Cheung Leung
Man Chun Li
Man Ting Mandy Ng
Kar Chiu Wong
Ka Ho Yau
Chin Keung Yiu

Ireland

Daniel Cookman
Florimon Giacobi

Japan

Ryosuke Hamagashira
Kenji Inoue
Koji Kashima
Kohsuke Kurashige
Ryan McNabb
Yasuhiro Morishita
Masashi Ono
Rui Tahara
Junichi Takeda
Kiyonobu Ueda
Hiroshi Yamashita

Jordan

Ahmad Abu Al Rub
Bara Al Hihi
Esraa Al Momani
Ahmad Aref AL-Dweikat
Nayef Hashem Al-Hussein
Laith Ensour
Mohaned Zaki Hamdan
Lubna Saleh Sawan
Ahmad Tarteer

Kuwait

Ali Jafaar Ghuloum

Latvia

Viktorija Intezare
Arturs Loze

Liechtenstein

Eliane Dandolo
Sigrid Rauch

Lithuania

Ramune Abazoriene
Ausra Kuoryte

Luxembourg

Klaus Peichl
Geng Zhou

Macau

San Hong Kuok
Wai Kin Lo

Macedonia

Elena Stojkovska

Malyasia

Verghese Panackel Peter

Mauritius

Khushal Kashish Phullah
Bibi Zaina Ramjaun

Mexico

Ernesto Luis Villalpando Fernandez

Netherlands

Evelyn Bell
Christine Gacheru
Ruben Paniry
Sahismail Pasaoglu
Ecem Uysalli
A.E.J. van de Plasse
Glynis van Leem
Arie van Walravena

New Zealand

Vanessa Adamson
Sheetal Bhardwaj
Uzair Rasool
Jeremy Williams
Danny Fan Yang

Norway

William Huy Duc Nguyen
Michael Torrissen

Pakistan

Babar Najam Khan

Romania

Teodora Oltean Gocan

Russia

Timur Borenshtein

Saudia Arabia

Mishal Saud Aljuleifi
Moustafa Conelly
Guan Wang

Singapore

Kien Pin Chen
Stanley Cheng Hwang Chew
Gabriel Foo
Damen Hee Peng How
Ong Yuemei Joy
Shirley Xue Ling Lam
Colin Yong Da Lim
Weixiang Jason Lim
Kian Mun Ng
Don Jason Lou Pastoral
Jia Qi Tan
Jonathan Weisheng Toh
Jared Wee Wen Wee

South Africa

Lize Mary Els
Oliver Jonathan Hill
Inna Podsekina
Bianca Wright

South Korea

Jaewoo Cho
Sukjin Chung
Su Yen Jin
Myoungshin Kim
Hyounjoo Lee
Boyul Son
Eun Im Yang
Seong Ryeong Yang

Spain

Juan Antonio García

Sri Lanka

Dona A. N. S. Muthukudaarachchige

Sweden

Hella Overhage

Switzerland

Jurgen Egberink
Matthias Greiller
Dimitrios Tsiolis

Taiwan

Chiao Fang Chen
Yu Hao Hsu
Ching-Yi Lin
Yung-Ju Lin
Pei Ling Tsai
Yu-Chien Wang
Chih-Chieh Wei
Wan-Hsien Wu

Thailand

Teeranan Pakariyasatid

Trinidad and Tobago

Andrew Dalip

Turkey

Ozan Guzel

Ukraine

Yuliia Kucheriava

United Arab Emirates

R M Ramith Bandara Ranathunga
Christos Christou
Lesleigh Groos
Sameer Hamza
Sushan S K
Mohanamanikandan Marimuthu
Sashidharan Menon
Moiz Patel
Muhammad Rashid
Nagarajan Thangavel
Murali Raj Vinayagam

United Kingdom

Bhavesh Desai
Loredana Ferri Di Fabrizio
Jon W. Harvey
Sofia Khan
Gustavo Mazuryk
Marzieh Pooladireishahri
Haleem Rana
Conrad Rhodes
Azliyaton Zainol

United States

Genevieve Abel
John Beauchemin
Stefanie Benner
Aditi Bidaye
Rowshanara Biswas
Erin Brackenridge
Peter W. Brinton
Dorothea M. Burke
Kristine Faith Cangcuesta
Danielle Nicole Carroll
Yangjingjing Clark
Delia Curshamer Compton
Javier Coronado
Sarah L. Costello
Tobias J. Cruz
Duc Truong Hong Duong
Jerome P. Evrard
Tiffany Gaines
Esther Geraci
Austin C. Geraghty
Benjamin Grier
Anna Hanson
Jennifer M. Hanson
Nadia Harold
David M. Hegge
Helen Elizabeth Hester
Trenton Julian
Jee Eun Jung
Da Yea Kang
Se Hwa Kim
Soojin Kim
Paulina Kojlo
Samuel Krivin
Adriana Krzeminska
Kai Ho Raymond Lam
Rui Li
Douglas E. Lippert
Lijuan Liu
Nialanda Lloyd
Peggy Ma-Baranovskiy
Chandrakant Maheshwari
Alejandro Malagon
Jamie Marshall
Emma Martin
Ryan B. McGrath
Natalie J. Monteil
Tetyana Morgan
Jorge Alberto Muñoz
Rebekah Nichols
Ifeanyi Nnoham
Kelly O'Donnell
Yoshihiro Okumura
Fernando Pardo
Katlynn M. Pentecoste
Anita Bibbs Piper
Jeffrey Pratt
Allison Elizabeth Raley
Beatriz Rincon Young
Rachel C. Rogers
Hewei Ruan
Shikhar Sahu
Eric M. Scofield
Umamani Selvam Sukumar
Jyotsna Sharma
Mohammad Majed Shatnawi
Junjian Situ
Eric A. Sohn
Ingo Steinhaeuser
Jihyung Sur
Haik E. Ter-Nersesyan
Michael D.K. Thompson
Louie Vargas
Donna Marie Vazquez
Theresa J. Von Dauber
Yichuan Wang
Alex Yevsyugov

Vietnam

Jaehong Park

The Power of a **Risk-based Approach in Sanctions & PEP Screening**

How granular can you get with your matching rules?

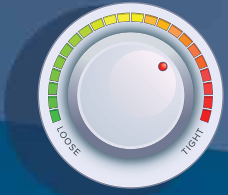
MATCHING RULE SCENARIOS

MORE GRANULAR

"One Size Fits All"

- Same matching rules for all Sanctions and PEPs

Risk-based Approach



- **Loose** rules on Sanctions
- **Tight** rules for all PEPs

27%

REDUCTION IN FALSE POSITIVES
vs. "one size fits all" approach

FinScan's Granular Risk-based Approach

- **Loose** rules on Sanctions
- **Loose** rules on high-risk PEPs
- **Tight** rules on low-risk PEPs
- **Exclude** expired PEPs, non-relevant PEPs
- **Use** secondary identifiers

87%

REDUCTION IN FALSE POSITIVES
vs. "one size fits all" approach

FinScan®
BY INNOVATIVE SYSTEMS

Advanced AML/KYC Solutions

Contact FinScan today to reduce your risk and false positives! | finscan@innovativesystems.com | **www.finscan.com**