

The magazine for career-minded professionals
in the anti-money laundering field

Ransomware: The digital battleground

ALSO IN THIS ISSUE:

September 11:
The 20-year journey





**The power to see
what's ahead.**

Get immediate risk insights in just one search with CLEAR.

Confidently and quickly verify identities, detect fraud risks, and research subjects and businesses in a matter of minutes. Thomson Reuters® CLEAR provides a comprehensive collection of public and proprietary records, sophisticated analytics, and transparent data in a single platform.

The data provided to you by CLEAR may not be used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or for any other purpose authorized under the FCRA.

Learn more at
tr.com/clear

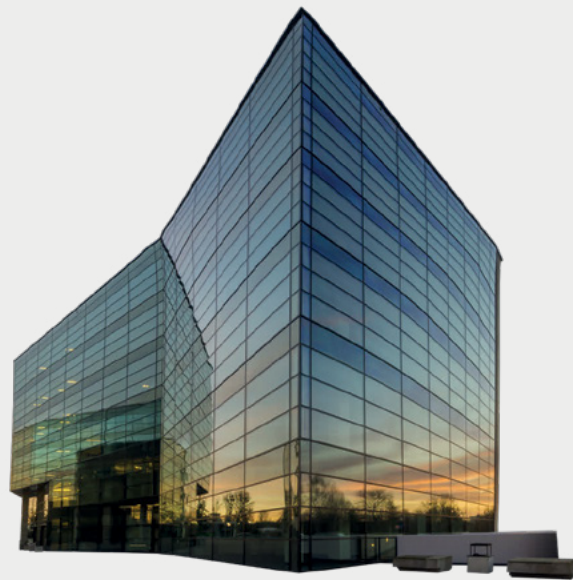
Visit us at our booth | ACAMS Las Vegas 2021



BUREAU VAN DIJK

A Moody's Analytics Company

Some see just a business



To us it's a subsidiary that's part of a corporate group
with 712 entities, linked to two PEPs,
and 'sanctioned by extension'



Welcome to the business of certainty

Request your free trial at [bvdinfo.com](https://www.bvdinfo.com)
to learn how our solutions help to deliver
new levels of certainty on your third parties

DIRECTOR OF EDITORIAL CONTENT
Kieran Beer, CAMS

EDITOR-IN-CHIEF
Karla Monterrosa-Yancey, CAMS

EDITORIAL AND DESIGN

EDITOR:
Stephanie Trejos, CAMS

INTERNATIONAL EDITOR:
Monica Mendez, CAMS

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
Ari Redbord
Joe Soniat, CAMS-FCI
Amy Wotapka, CAMS

SENIOR LEADERSHIP TEAM

PRESIDENT AND MANAGING DIRECTOR:
Scott Liles

VP OF PROGRAMME DEVELOPMENT AND MARKETING:
Angela Salter

GLOBAL HEAD OF HR:
Bill Lumani

VP OF GLOBAL SALES:
David Karl

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

VP OF GLOBAL STRATEGIC COMMUNICATIONS:
Lash Kaur

VP OF FINANCE AND GLOBAL OPERATIONS:
Mariah Gause

SR. DIRECTOR 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
William D. Langford, CAMS
Dennis M. Lormel, CAMS
Rick McDonell, CAMS
Karim A. Rajwani, CAMS
Anthony L. Rodriguez, CAMS, CPA
John Smith

ADVISORY BOARD (continued)

Daniel D. Soto, CAMS
Dan Stipano
Philippe Vollot

STAFF CONTRIBUTORS

AML DIRECTOR—EUROPE, MIDDLE EAST AND AFRICA:
Shilpa Arora, CAMS

SENIOR DIRECTOR, AML OF AMERICAS
Lauren Kohr, CAMS-FCI

REGIONAL AML DIRECTOR APAC:
Rosalind Lazar, CAMS

DIRECTOR, AML—CHINA:
Lynn Li, CAMS

SALES AND REGIONAL REPRESENTATIVES

SENIOR VP 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

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 Today © 2021 published by ACAMS. All rights reserved. Reproduction of any material from this issue, in whole or in part, without express written permission of ACAMS is strictly prohibited.

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.

LOOKING FOR MORE ACAMS TODAY CONTENT?

Visit ACAMSToday.org!



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

It's time for **SMARTER, FASTER FRAML**

NICE
ACTIMIZE

Harness the power of best-in-class AI, data intelligence, analytics, and insights within a single cloud-native platform.

The Xceed logo is centered within a circular graphic that has a white-to-pink gradient. The word "Xceed" is written in a bold, black, sans-serif font. The "X" is significantly larger than the other letters. A blue cloud-like shape is positioned above the "ce" and below the "d".

Xceed

It's time to work smarter, not harder. > niceactimize.com/xceed

CONTENTS

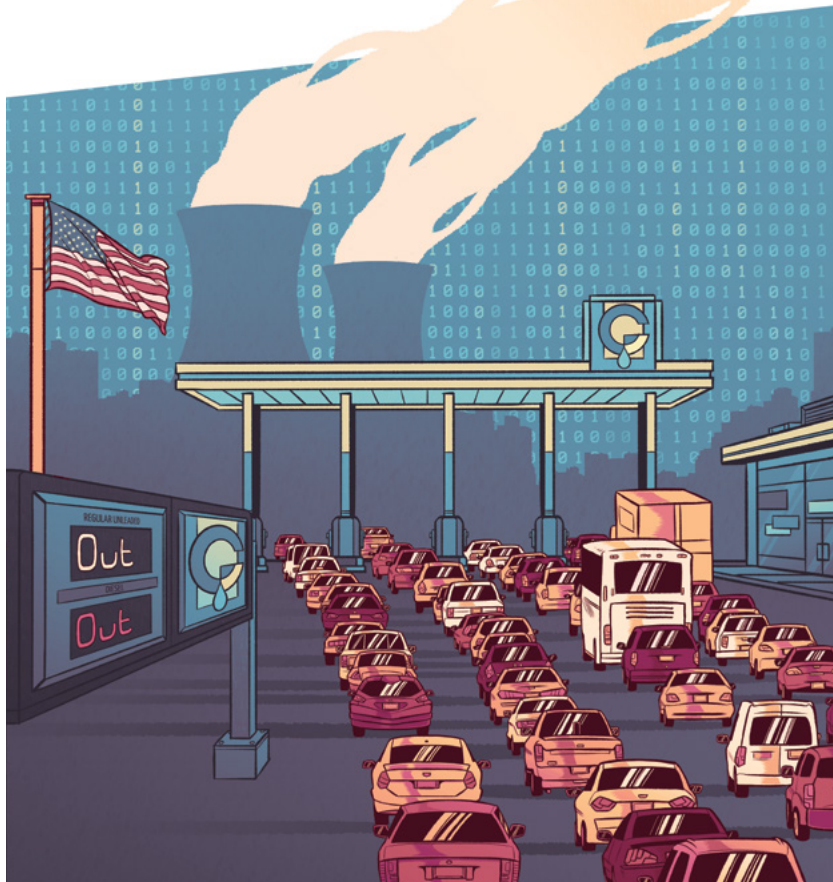


Illustration by: Milos Hall

ON THE COVER:

56

Ransomware: The digital battleground

A case study of the Colonial Pipeline ransomware attack and its larger implications on AFC professionals.

8
From the editor

10
Member spotlights

12
A message from the director of editorial content

14
Nonprofits: Know your donor's asset origination

The growth of donor-advised funds could lead to money laundering in the NPO sector.

18
Riddle me this: Export controls?

Breaking down the what, where, why and to whom of export controls.

22
Cryptocurrency exit scams—What they are and how to avoid them

Defining cryptocurrency exit scams and how to protect oneself from them.

26
Data's impact on compliance and AFC operations

What are the consequences of not being able to manage data properly?

28
The nexus between ransomware, cryptocurrency and money laundering

As ransomware becomes a greater threat, criminals have begun using cryptocurrency as the medium of exchange to launder their funds.

32
Casinos and the why of money laundering

To catch a money launderer, casino personnel must think like a money launderer.





38

**38
Strengthening your DPMS toolkit**

Diving into the many opportunities the jewelry industry provides for money laundering.

**42
A guide to surviving an audit**

An audit survival checklist for preparation, management and post-audit actions.

**46
Best crisis management practices for data breaches: Part one**

Ways your financial institution can prevent and prepare for a data breach.

**50
The right data for KYC success**

AML professionals must look beyond the collection and collation of individual data elements.

**54
Twenty impacts over 20 years**

ACAMS advisory board co-chair Rick Small and former advisory board member Lauren Kohr provide top 20 changes in the AML space throughout ACAMS history.

**62
September 11:
The 20-year journey**

The history of 9/11 and its continued impact on AFC.

**66
Elder financial exploitation:
A monumental crisis**

A law enforcement perspective on tackling elder financial exploitation.

**70
The new whistleblower program
AML professionals should know**

Details on the AMLA's expansion of the BSA whistleblower program.

**74
The European cybersecurity ecosystem: A war on cybercrime**

A review of Europe's latest proposals, guidelines, strategies and legislation to combat cybercrime.

**82
Analyzing South Korea's
'Nth Room' case**

Bringing awareness of digital sex crimes and modern slavery through the lens of the Nth Room case.

**92
Musings after quarantine
chapter 3: Job seekers
strike back**

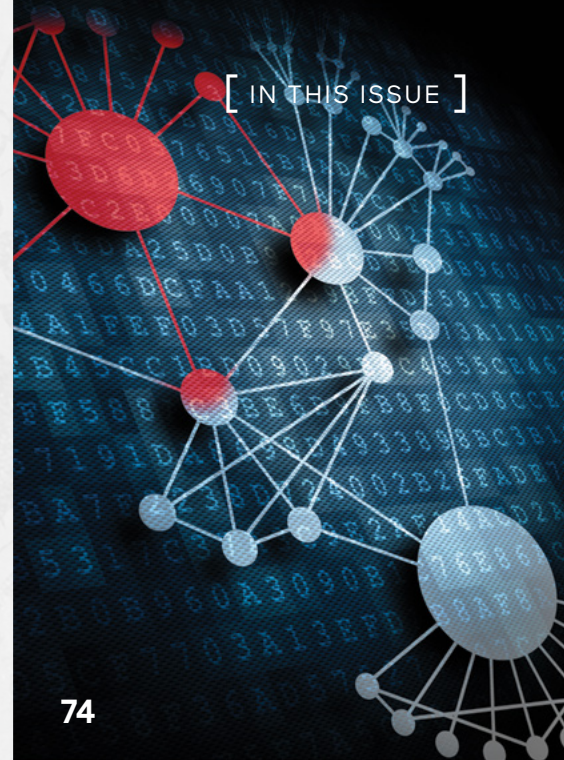
How job seekers can take advantage of the pandemic recession ending.

**96
Making event trigger
reviews work**

How to make event trigger reviews more effective in managing a financial institution's client risk.



62



[IN THIS ISSUE]

74

ASPECTS OF APAC

**88
How to incorporate money
laundering risk into risk
management: Part one**

How to evaluate and measure the loss caused by the money laundering risk.

KNOW YOUR CHAPTER

**100
Greater Phoenix Chapter:
Pivot, evolve and adapt!**

A recap of the Greater Phoenix Chapter's event on terrorist financing in the crypto age.

**102
Meet the ACAMS Staff:
Winnie Yuen**

**104
Advanced Certification
Graduates**

**106
CAMS Graduates**

**117
CGSS Graduates**

Reflections of 9/11

This year marks the 20-year anniversary of the worst terrorist attack on U.S. soil. We all remember where we were when we heard the news. I was living in the Rocky Mountains and had just jumped into my car to head to work. I had the radio on and heard that a plane crashed into the Twin Towers. At first, I thought is this a mistake? I then switched to a different station, heard the same report and drove to work in shock. As soon as I arrived, I saw the same shock reflected in my co-workers' eyes. We all huddled around our computer screens frantically trying to get more updates and to understand what was happening. We saw the second plane crash into the Towers and then the collapse of the South Tower. I had a co-worker who had a family member flying and she was anxiously trying to find out what happened to her plane. The world sat in disbelief and everyone I knew started asking the same questions. How could this have happened on U.S. soil? Were there no warning signs? How were we not prepared?

Without question, 9/11 had far-reaching effects across multiple aspects of our lives. In particular, it changed the banking industry and all financial institutions. September 11 brought about the USA PATRIOT Act, the most transformative regulation of its time. Anti-money laundering (AML) and terrorist financing (TF) were at the top of everyone's list. Collaboration across the public and private sectors was now needed to succeed in combating money laundering and TF, along with improvements in record keeping and know your customer requirements. The most significant accomplishment of the PATRIOT Act was to facilitate the process of detecting and deterring TF, not only in the U.S., but on a global scale.

As we reflect on what has happened in the last 20 years since 9/11, not only in the compliance industry but in the world at large, the question is have we progressed in our fight against financial crimes? I believe we have. I believe the industry is constantly evolving and as ACAMS' members or anti-financial crime professionals, we are doing our part to continue the fight against money laundering and TF. The fight against bad actors has evolved due to new technology, but the goal is still the same—defeat the “bad guy.” The headline article “Ransomware: The digital battleground” addresses one of our biggest threats today—cybercrimes. The article dissects the Colonial Pipeline as a case study and one of the most poignant phrases in the article comes after the U.S. Justice Department elevated cyber-intrusions to be as important as counter-terrorism investigations. The author states,

“This shift by law enforcement could signify the first shift in national security policy in over 20 years—a recognition that this is now a post post-9/11 moment where terrorists, cybercriminals and rogue nation state actors have taken to the digital battlefield.”

Clearly, we have come a long way in 20 years, but there is still much to do.


ACAMS is also celebrating 20 years of existence so *ACAMS Today* asked two of our leading subject-matter experts, a board member and a former, Rick Small and Lauren Kohr, to share with us their top 20 list of transformative events that have shaped the anti-financial crime industry in the last two decades. It is of no surprise that the events of September 11, 2001, was at the top of their list. Read



more about their thoughts and what they predict will be at the forefront in the years to come.

Our annual conference edition is packed with content ranging from the new whistleblower program to cryptocurrency exit scams, the impacts of 9/11, export controls, donor-advised funds, casinos and money laundering, surviving an audit and a plethora of more topics.

We hope you will join us as we begin celebrating 20 years of ACAMS. These festivities will continue throughout the year and into 2022 with the additional celebration of 20 years of *ACAMS Today* in the March-May 2022 anniversary edition. Watch this space for more details about upcoming celebration plans.

May we all take a moment during the 9/11 20-year anniversary to remember and honor those who lost their lives on this tragic day. May we also remember and honor the first responders who on that dreadful day ran toward danger to save lives even at the cost of their own. 

Karla Monterrosa-Yancey, CAMS editor-in-chief

Follow us on Twitter: @acamstoday



Connect with Abrigo at ACAMS Las Vegas 2021



Visit the Abrigo Booth (431 & 433) for
your chance to win 1 of 3 iPad Giveaways.

We will have a new winner each day, giving
you three chances to win!



TERRI LUTTRELL
Abrigo



VANESSA RUSSELL
Love Never Fails



TISH LEON
Love Never Fails

You will not want to miss our session – *Justice for Victims of Human Trafficking...One transaction at a time.*
from Abrigo's own Terri Luttrell, and Vanessa Russell and survivor Tish Leon from Love Never Fails.

Monday, September 27 | 11^{AM}



BSA/AML



Fraud Prevention



Advisory Services

Abrigo enables more than 2,500 U.S. financial institutions to support their communities through technology that fights financial crime, grows loans and deposits, and optimizes risk.

Ready to get started?

Visit www.web.abrigo.com/ACAMS-Las-Vegas



**Sandra Edun-Watler, CAMS
Cayman Islands**

Sandra Edun-Watler is an attorney-at-law and the head of the compliance and reporting services for Mourant Governance Services in the Cayman Islands. In this role, she provides anti-money laundering (AML) and automatic exchange of information reporting as well as compliance officer services to Cayman Islands entities.

Edun-Watler was previously legal counsel with the Cayman Islands Monetary Authority before joining Walkers, the global law firm. While at Walkers, she held numerous positions including head of compliance with responsibility for the Cayman Islands, British Virgin Islands and Bermuda offices. She also advised clients in her role as a regulatory lawyer and was instrumental in the setup and launch of the AML officer services business line.

Edun-Watler has a wealth of knowledge and practical experience from all aspects of the AML and compliance function. She is the president of the Cayman Islands Compliance Association, deputy chair of the AML Steering Group of the Cayman Islands Legal Practitioners Association, and member as well as former chair of the Caribbean Regional Compliance Association. In addition, Edun-Watler was the legal assessor for the Caribbean Financial Action Task Force's third round of mutual evaluations for the British Virgin Islands. She also guest lectures on AML at the Truman Bodden Law School and sits on various working groups representing the Cayman Islands Compliance Association.



**Muhammad Rizwan Khan, CAMS-FCI,
CGSS, CTMA, CKYCA
Pakistan**

Muhammad Rizwan Khan was recognized for his dedication to the anti-financial crime field. Khan has achieved several compliance certifications from ACAMS, including Certified Anti-Money Laundering Specialist (CAMS), Certified Transaction Monitoring Associate (CTMA), Certified Know Your Customer Associate (CKYCA), Certified Global Sanctions Specialist (CGSS) and Advanced CAMS-Financial Crimes Investigations (CAMS-FCI). He is currently a student at the University of Oxford Saïd Business School and is enrolled in their diploma in the organizational leadership program.

Khan is currently the general manager for the Al Dhahery Money Exchange in the United Arab Emirates. In this role, he is tasked with implementing best practices for detecting and preventing financial crime.

Khan has vast experience in AML and counter-terrorist financing. He is a compliance professional with a focus on financial crime and independent money laundering reviews for the money services business industry and banks. His expertise also includes independent reviews and investigations, threat/risk assessments, domestic and international training, mentorship, expert testimony and AML program development. Khan has written articles that have been published in numerous academic international compliance forums and he is recognized as one of the world's leading experts on the subject.




**Howard Spieler, CAMS
NY, USA**

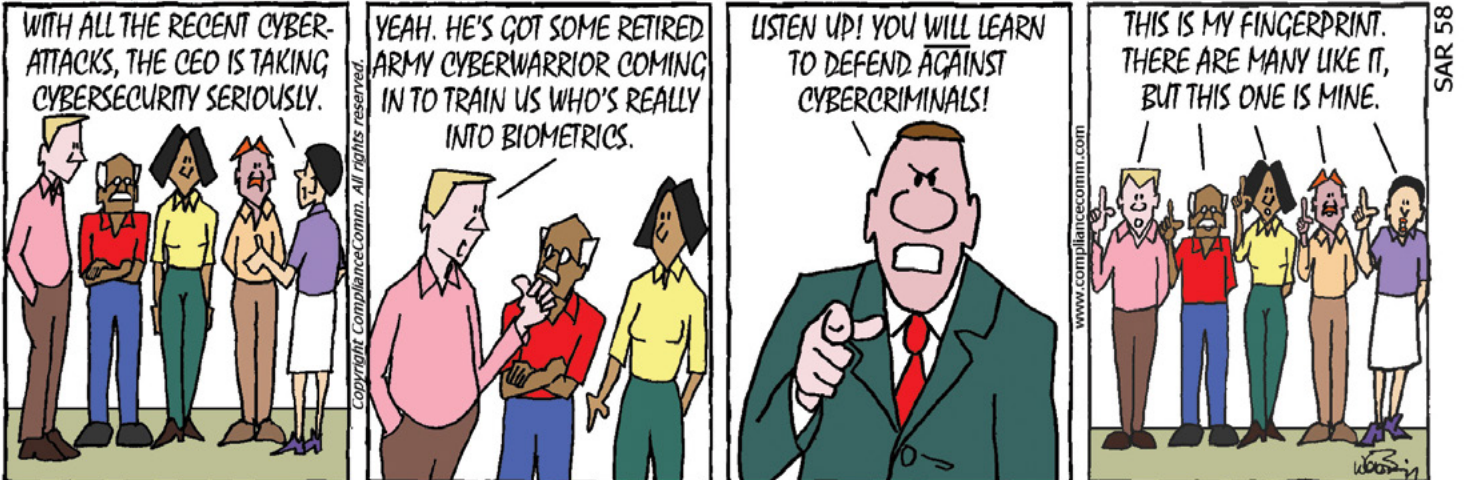
Howard Spieler, co-chair of the ACAMS New York Chapter, has nearly 20 years of compliance-related experience. Throughout his career, he has provided guidance and oversight to businesses and other stakeholders on their applicable legal, regulatory and policy requirements in anti-financial crime and other compliance risk areas.

Currently a vice president for the global sanctions compliance department at MUFG, Spieler serves as a sanctions subject-matter expert supporting various programmatic initiatives, including risk assessments as well as domestic and global product reviews. Previously, he held anti-financial crime roles at Citibank and AIG, where he provided subject-matter expertise to global stakeholders.

Before that, Spieler served in the Bloomberg administration for 10 years, with seven of those years as head of compliance at the New York City Economic Development Corporation, where he helped develop and maintain its risk-based compliance program. He was responsible for the ongoing monitoring and assessment of a \$30 billion portfolio of public-private real estate transactions, which included managing regulatory reporting.

Spieler authored “A Global Review of Sanctioned Countries” and “The Impact of the U.S. President on Economic Sanctions,” which were both published by *ACAMS Today*. He is a Certified Anti-Money Laundering Specialist (CAMS) and Certified International Sanctions Compliance Officer (ISCO). Spieler holds a master’s in accountancy from Kean University, a Master of Business Administration from St. John’s University and a Bachelor of Arts with a focus on political science from the University at Albany, State University of New York. 

SARSnSTRIPS™



Twenty years later: What we lost, what we gained

Most of us can vividly recall where we were 20 years ago on September 11, 2001.

At 8:46 a.m., the North Tower of the World Trade Center was struck by what many initially assumed was a small off-course plane. But when the South Tower was struck at 9:03 a.m., it became clear that America was under attack.

Surrounded by wall-to-wall screens at *Bloomberg News* in midtown, Manhattan, I fell to my knees when I saw the South Tower collapse at 9:59 a.m. A woman assigned to greet visitors ran to ask if I was alright. Yes, I was fine—but thousands of people had just been killed, I remember saying.

With a clear view of the lower Manhattan skyline from our home in Brooklyn, all my wife could see was a thick cloud of smoke where the Twin Towers had stood. Yet on the phone with her parents in Florida, she remembers saying “don’t be ridiculous” when her mother reported that one of the towers had fallen.

The North Tower fell at 10:28 a.m.

The nearly 3,000 who died that day represented different ethnicities, religions and socioeconomic classes as varied as America itself.

A former colleague recounts escaping across the Brooklyn Bridge with a huge crowd of people, many covered in soot and dust from the buildings. When jets roared overhead, everyone became more afraid until someone shouted, “they’re ours, they’re ours!”

At 9:37 a.m., a third plane crashed into the Pentagon and a fourth plane, headed for the Capitol Building or White House, crashed into a Pennsylvania field at 10:03 a.m. when passengers stormed the cockpit held by terrorists.

The world was changed by the attacks. But it was also changed by our response to the attacks.

In small and large communities throughout the country and around the world, and at every level of government, we came together.

In my neighborhood, friends did what they could to comfort one another, including helping families locate the missing. Hospital operators were unfailingly polite each time they were asked to check—and recheck—admittance logs.

And we watched as Republicans and Democrats, for the most part, stood united. By October, a bipartisan commission was created to learn lessons from the attacks, and the disparate proposals around financial transparency as well as the oversight that had previously hit political roadblocks were signed into law as part of the USA PATRIOT Act.

In this issue, Dennis Lormel, the first chief of the FBI’s Terrorist Financing Operations Section (TFOS), which was founded in the wake of 9/11, recalls the determination and unity around countermeasures to terrorism, not least the creation of public-private partnerships for information sharing.

The birth of those partnerships coincided with the conception of ACAMS. A small media and conference organization, Alert Global Media, embraced the idea of credentialing anti-money laundering and counter-terrorist financing professionals and creating a professional association that would serve as a hub of information and a platform for sharing new ideas and best practices. Now, with more than 83,000 members globally, ACAMS will celebrate its 20th anniversary in the




March-May 2022 issue of *ACAMS Today*. Look for more information about the celebrations in the editor-in-chief’s letter.

Lormel, as he has throughout his law enforcement career, his subsequent tenure as a consultant and his involvement with ACAMS as an advisory board member, makes a plea that we maintain the shared sense of urgency and diligence against terrorism that was inspired by our shared experience of 9/11.

That plea takes on a new poignancy with the return of the Taliban to power in Afghanistan and the rise of new terrorist threats, including from domestic extremists, particularly racially or ethnically motivated violent extremists (RMVEs).

Today the U.S. and indeed the entire world is not as unified in indignation against terrorism as it was post-9/11, although some important alliances forged then remain strong.

But this only makes the call to diligence and ACAMS’ global mission all the more important as we look back on what we lost on 9/11 and what we gained when we came together. 

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

Is your AML/CTF compliance easy and automated?

Remove manual processes and revolutionise your AML/CTF reporting with our end-to-end compliance automation platform.

Transform manual processes into secure digital workflows, for a complete and accurate view of transaction information, faster payments, and reduced financial crime compliance risk.

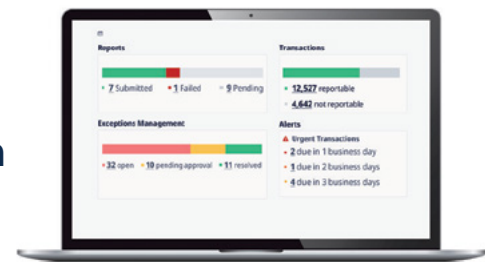
Automate payment investigations

Reduce the risk of financial crime compliance by automating how you identify missing KYC/CDD information for in-flight transactions and by securely requesting and sharing data and documents internally and with customers.

Streamline regulatory reporting

Simplify your AML/CTF reporting with a single platform that lets you easily identify reportable and non-reportable transactions, remediate exceptions and report directly to the regulator.

Book your free demo today. Visit identitii.com



NONPROFITS: KNOW YOUR DONOR'S ASSET ORIGINATION





Illustration by: Joya Jones

When learning about new trends in money laundering from financial crime prevention experts, one usually does not consider the nonprofit sector and the risk of nonprofit organizations (NPOs) in facilitating illicit transactions.

Nonprofits are essential to financing the most vulnerable in society; however, they could become a target for sophisticated money laundering schemes due to the lack of know your donor (KYD) policies and the recent growth of complex asset gifting within donor advised funds (DAFs).

Know your donor-advised funds

One type of tool that is growing in popularity within the NPO world is the donor-advised fund, more commonly known as the DAF. According to Fidelity Charitable,¹ DAFs are the fastest-growing charitable giving vehicle in the U.S. due to the ease of creation and their tax-advantageous ways in gifting to charity.

With donors enjoying current favorable tax code structures within gifting deductions, and the ability to retain advisory rights and recommendations of the assets, DAFs are seeing a consistent increase in popularity. According to the National Philanthropic Trust,² assets jumped 16.2% between 2018 to 2019 from \$122 billion to \$142 billion. Barrons recently reported that the number of DAFs rose roughly to 873,228, rising 19.4% between 2018 and 2019 and rising over 300% in the last 10 years.³

DAF assets and accounts are growing rapidly at 15%-20% annually and so is the sophistication of how donors give through complex assets. According to the National Philanthropic Trust, the DAF world is seeing an increased interest in illiquid contributions.⁴ With more foundations and sponsoring organizations creating their own in-house DAFs, there is a higher likelihood of unethical donors using smaller and overlooked foundations to fund other illicit nonprofits (those that lack a KYD policy).

Complex assets complicate due diligence

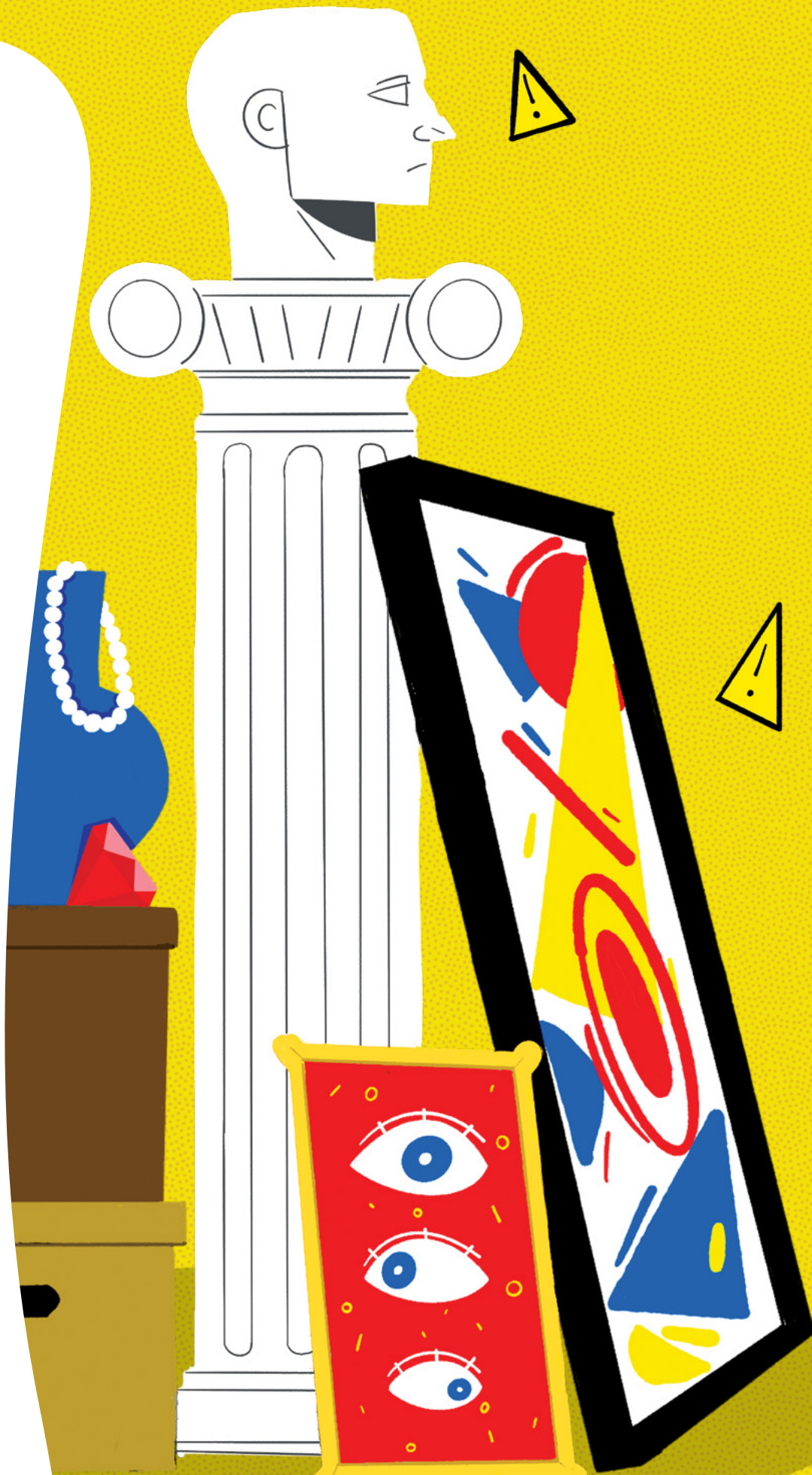
More complicated financial instruments—such as cryptocurrency and illiquid private funds—are being introduced to the NPO world. In 2017, the National Philanthropic Trust's DAF⁵ reported a rise within noncash contributions. From the 60% of contributed assets studied in 2017, 60% of those assets were noncash-related. These assets include public and nonpublic securities, real estate and even fine art.

These complex and alternative asset gifts are posing higher risks of being misunderstood, unvetted and passed through NPOs.

Case study

The following is an example of how minimal vetting of a DAF asset could uncover a modern-day tax evader, or even worse, a terrorist financier.

The donor is a business owner who has enjoyed the success of his private enterprises. Since NPOs survive on gifts of assets, NPOs are more likely to accept gifts of vast asset classes and structures to further their nonprofit mission for societal gains. This donor in particular wishes to give an alternative asset, such as a complex offshore and onshore hedge fund from his private bank, to the foundation. His intent is to receive a gift deduction and have the ability to advise the DAF on where the asset should be ultimately gifted. The DAF provider accepts this gift with minimal knowledge of anti-money laundering and counter-terrorist financing measures and becomes a legitimate middleman for the donor's potential illicit transactions. As the donor knows, the recipient of the asset is the DAF provider itself since the asset is now owned by the foundation and out of the donor's name. This allows the donor to place a complex asset, out of his name, into the financial system, creating more complexities and layers to further himself from his potential illicit transactions.



Financial Action Task Force guidance

In October 2002, the Financial Action Task Force (FATF)⁶ responded to the 9/11 terrorist attacks in the U.S. with best practices on combating the abuse of NPOs after high-risk NPOs were found to be more commonly facilitating illicit transactions. Recommendation 8 of the FATF 40 Recommendations was created to bring more awareness on how nonprofits could be used in the world of terrorist financing.

In 2014, FATF conducted a third round of evaluations⁷ to see if jurisdictions were within compliance of Recommendation 8. During this evaluation, FATF found that 57% of these higher risk jurisdictions were either not compliant or were only partially compliant with Recommendation 8. Only 5% of those evaluated were fully compliant or largely compliant.

The Financial Crimes Enforcement Network's recent guidance on customer due diligence for nonprofits and charities

In November 2020, the Financial Crimes Enforcement Network, along with U.S. federal banking agencies, issued a helpful fact sheet⁸ that reminds commercial banks to apply a risk-based approach to charities and other NPOs. It is important to note that the U.S. does not consider the whole nonprofit sector as "high risk." However, regulators do urge financial institutions (FIs) to consider how donors are being vetted.

Steps nonprofits can take

As regulatory bodies note, charities and nonprofits should make sure that KYD policies are in place. In today's growing nonprofit world, NPOs should not only depend on the FI's know your customer (KYC) program.


Nonprofits can be the first line of defense by investing more resources in a KYD policy and formal due diligence procedures before accepting complex gifts.

The following questions are a starting point for nonprofits to consider when creating a KYD policy:

- Where is the donor geographically located?
- Who are the current beneficial owners?
- Is the donor currently on the Office of Foreign Assets Control Specially Designated Nationals list?
- How will the gift be structured?
- What is the purpose of the gift?
- Who will be the end recipient of the gift?
- Does the donor intend on gifting assets to nonprofits with operations overseas?

If the nonprofit finds that the donor is evading these simple KYD questions, the NPO should conduct enhanced due diligence before accepting the gift. This simple due diligence can protect the nonprofit's integrity and strengthen its reputation.

In conclusion

As bad actors learn more about the ever so popular DAF and the anonymity that they operate in, there will be potential for more illicit transactions and the integration of ill-gotten gains. NPOs can protect themselves and the vulnerable they serve by asking more asset origination questions and conducting due diligence when higher risks are detected. 

Josh Ortner, CAMS, OH, USA

¹ "What is a donor-advised fund?" *Fidelity Charitable*, <https://www.fidelitycharitable.org/guidance/philanthropy/what-is-a-donor-advised-fund.html>

² "The 2020 DAF Report," *National Philanthropic Trust*, 2020, <https://www.nptrust.org/reports/daf-report/>

³ Abby Schultz, "Donor-Advised Fund Assets Reach \$142B, Grantmaking Hits \$27B" *Barrons*, February 2, 2021, <https://www.barrons.com/articles/donor-advised-fund-assets-reach-142b-grantmaking-hits-27b-01612298241>

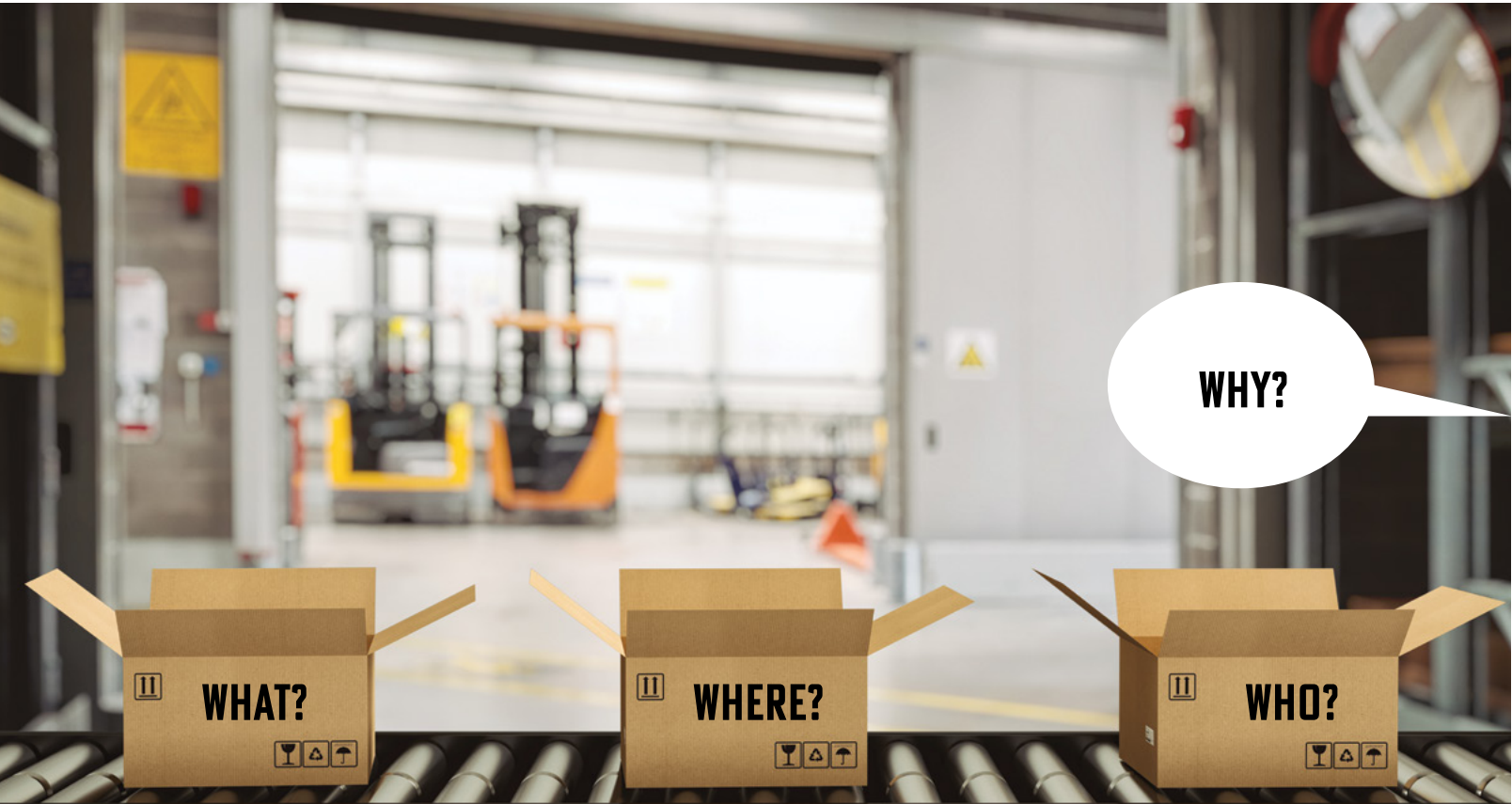
⁴ "2020 Donor-Advised Fund Report: Grants to Charities Increase 15% to \$27 Billion and Total Charitable Assets Surpass \$141 Billion," *Business Wire*, February 2, 2021, <https://www.businesswire.com/news/home/20210202005410/en/2020-Donor-Advised-Fund-Report-Grants-to-Charities-Increase-15-to-27-Billion-and-Total-Charitable-Assets-Surpass-141-Billion>

⁵ Eileen R. Heisman, "Findings from our 2018 Donor-Advised Fund Report," *National Philanthropic Trust*, December 3, 2018, www.nptrust.org/philanthropic-resources/philanthropist/findings-from-our-2018-donor-advised-fund-report/

⁶ "Best Practices on Combating the Abuse of Non-Profit Organisations," *Financial Action Task Force*, June 2015, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html>

⁷ "Risk of Terrorist Abuse in Non-Profit Organisations," *Financial Action Task Force*, June 2014, <https://www.fatf-gafi.org/media/fatf/documents/reports/risk-of-terrorist-abuse-in-non-profit-organisations.pdf>

⁸ Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations," *Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency*, November 19, 2020, www.fincen.gov/sites/default/files/shared/Charities%20Fact%20Sheet%2011_19_20.pdf



RIDDLE ME THIS: EXPORT CONTROLS?

As governments seek to accomplish national security and foreign policy goals, the regulatory focus has increasingly turned to export control compliance. Controlling goods for export has long been a tool used by government leaders to keep dangerous products, such as weapons and chemicals, out of general distribution and strategic goods, such as supercomputers and advanced electronics, out of the hands of one's adversaries. Over time this has created a high stakes regulatory patchwork to be deciphered and followed, much like solving a riddle. Merriam-Webster defines a riddle as "a mystifying, misleading, or puzzling question posed as a problem to be solved." A characterization that many financial compliance practitioners may use to describe export controls; however, export controls need not feel so daunting. Irrespective of where a shipment is coming from or where it is going, there are always four export control riddles to be solved: What is the product, where is it going, to whom and why?

Export controls in layman's terms

No citizen or company of any country in the world has the right to export, absent a prima-facie right to do so—export permission is required from the government. On the other hand, no government wants to expend the time and resources reviewing export permission requests for all transactions. In response, governments build export control rules, which quite literally are designed to control the flow of exports from their country. This collective body of export rules and suggested best practices represents a government's attempt to strike a balance between controlling exports, products, technology and services that are “dangerous” and those that are not. If an item is controlled, an export permission is needed, but only under certain circumstances. Governments leave it to the exporters to figure it out for themselves under what circumstances they need not ask the government for an export license and when they need to based on the full body of export rules.

After explicit permission is requested and granted in the form of an export license, the circumstances wherein an exporter can move forward with a transaction is both continually evolving and dramatically changing. As commercial and dual use products develop, mature and become publicly available, export controls evolve in response. They also change, sometimes quite dramatically, in response to concerns around crime control, foreign policy, national security, domestic economics and, of course, political optics. Export regulations, statutes and legal precedent are tens of thousands of pages in length, full of mystifying, occasionally misleading content and certainly with puzzling details as to the requirements. These must be collectively understood and acted upon, which is the role of global



trade compliance managers, directors and their staff. For everyone else tangentially involved in export control compliance, what may seem mystifying, occasionally misleading and certainly with puzzling details can be distilled to four simple riddles. Understanding how to solve these riddles is the key to understanding export controls.

Riddle #1: What is the product being exported?

The type of product being exported is significant to solving the first export control riddle. If shipping paper clips, rulers or other office supplies, there are no security concerns or foreign policy implications to those types of benign commodities. As a result, governments definitely do not want exporters to request an export license for a stapler. At the other end of the spectrum, there are the exact kinds of products—missiles, munitions, high-end computers and nuclear materials—for which the government expects a lengthy and detailed export license request. And then there are a whole lot of products in the middle such as medicine, electronics, batteries and many types of industrial goods. All physical items are either controlled or not controlled for export. In addition, most intangibles that support

controlled items are also controlled such as service calls, technical support, software, encryption and other technologies to keep the controlled item up and running. If an item, software or technology is controlled, it is classified for each country of export and assigned an Export Classification Number (ECN). The assigned ECN determines if an exporter's products are captured under an export license requirement. A product and its associated technology and services can also be released from an export license obligation under a byzantine maze of exceptions and exemptions. Know that the “catch and release” principle in export control compliance exists and that the operational implementation of this framework resides with the global trade compliance team. What is the product? The answer to this riddle is found in the item's ECN.

Riddle #2: Where is it going?

A significant aspect of understanding export controls is comprehending the risks associated with managing export control risk. Where an export is going is at least as important as the product itself. It warrants mentioning that just because an item can be exported, it does not mean that it can be imported upon arrival. Location-based export controls are unwieldy and come in the form of sanctions, embargos, treaty mandates, national and multinational country controls, and an organization's willingness to manage this type of risk in the first place. Some export destinations are so strictly limited that one would not bother to ask for an export license because shipping even noncontrolled office supplies are prohibited (think North Korea and Syria, and Cuba for U.S.-based exports). Excluding the most highly controlled goods, implements of torture and weapons of mass destruction, there are other countries with very few export

controls. In others, only certain regions carry an export license requirement such as the Republic of Crimea in Ukraine or specific addresses such as those found under sanctions published by the Office of Foreign Assets Control (OFAC) and international equivalents of OFAC. But most countries can be found in the middle, for which the need to obtain an export license depends upon the product (riddle #1) coupled with a dizzying set of multilateral and bilateral rules that an organization's global trade compliance team is responsible for deciphering. Shipments and transshipments to Iran frequently get large multinational commercial exporters into trouble, in part, because the Iranian Transaction and Sanction Regulations are difficult to figure out, making it difficult for compliance to manage. Finally, just to make the operational realities more challenging, many location-based export controls are in force irrespective of where the export is physically taking place. To counter the risk associated with this occasionally indecipherable swirl of rules, organizations enact their own country "embargo" controls based not just on the mandated government rules but also on reputation, diversion, credit and other operational risks the company is not willing to take. Where an export is going determines the export controls in effect, the answer to which solves riddle #2.

Riddle #3: To whom?

This is the export control riddle with which those in the financial crime prevention community are most familiar. Business partner and counterparty sanctions screenings, ownership structure analyses, state-owned entity reviews and military affiliation validations are part and parcel of solving the export control riddle much as they are for financial crime analysis. If an organization's due diligence process determines that a potential business partner's

financial supply chain or overall compliance posture is not up to par, participating in the physical supply chain with this partner is ill-advised. Government enforcement officials have been quite effective at getting this clear message out. But there is more to solving riddle #3 than meets the eye.


Office supplies, check. Sanctions screening, check. Export from the U.S. to Germany, check. To the German military—beep! The products and countries involved in this export transaction would not trigger a license requirement, and the buyer is not a sanctioned party, but the "to whom" is a military organization and that changes the effective export control rules for the transaction. While military end-user rules have been on the front page of compliance news as of late, validating government and military connections of an end-user has been an aspect of export controls for decades. Evaluating the type of business that an end user is associated with is cumbersome and time-consuming but often necessary to solving this export control riddle.

Riddle #4: Why?

Why is an orphanage in Brazil buying high-end supercomputers? Good question and exporting without finding out is done at one's own peril. Unless a red flag of a nefarious nature such as this occurs mid-transaction, most exporters do not need to find out why a product was ordered or how it will be used. Exporters are required to conduct a sanctions and restricted party screening, a military end-use check depending on the product and a country-based risk check by comparing the product's assigned ECN to a list of country destinations and obtaining an export license when applicable. Taking these steps solved the first three export control riddles. There is a fourth question that

rarely needed to be asked but in today's heightened compliance and risk mitigation climate, it should be asked more often. This can be true even when dual-use (commercial and military potential use) items are not involved in an export transaction. Why does the buyer want this item? What is the intended use? Does it make sense for them to purchase this item? In this quantity? From this company? How commercially intrusive and operationally disruptive the end-use vetting needs to be is subjective. And while this has been a way of life for military-spec and dual-use exporters, it is a new concept for most other exporters. The basics will always matter and the first three riddles must be solved: What is the product, where it is going and to whom are paramount. What is evolving and changing is how those factors combine and weigh upon one another in determining an end-use validation requirement. Stopping an export transaction to validate riddle #4 costs companies time and money and makes the already irreducible complexity of supply chains that much more so.

Those riddles were not too difficult, right?

Export controls are not as daunting as they might seem, although they are absolutely complex and chock-full of compliance risk. As with any risk-based compliance program, export controls are namely about striking a balance between keeping business moving and keeping it compliant. This is the overarching goal of a risk-based export control compliance program and the government's motivation in requiring organizations to have one. 

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

AML Just Got Smarter. And Faster.

Fight money laundering with intelligent automation.

The stakes are higher than ever. As money laundering and other financial crimes grow more complex, automating AML processes is imperative to staying competitive.

Discover how top financial organizations are using AI, machine learning and predictive analytics to increase automation - transforming their ability to flag cases, identify patterns, and analyze entire networks of criminals more quickly and efficiently.

Learn more at sas.com/iapaper





Cryptocurrency exit scams—

What they are and how to avoid them

Throughout the years, cryptocurrency has become a very controversial topic of discussion, mainly through the two opposing forces that try to navigate within the space. On the one hand, there are believers of the technology, the futurists and the innovators who buy bitcoin¹ and store it safely.

On the other hand, there are those who prey on the less educated, trying to take advantage of their lack of knowledge, and scam them into giving up their crypto. This happens in a multitude of ways and recognizing it can be tricky.

As the crypto space evolves, so do the methods of these so-called scams. The exit scam is one of the hardest to spot. So, what does the term mean and how can one avoid falling victim to it? This article defines the exit scams and gives suggestions on how to protect oneself from this type of scam.

What are cryptocurrency exit scams?

An exit scam refers to a cryptocurrency profiting from early investors by literally “pulling out” all their funds from the market. In other words, the people with the largest wallets of a specific new cryptocurrency try to artificially inflate (pump) the price through marketing and promotional activities, only to later get rid of their personal bags (dump) onto new investors.

Where do we find such scams?

Cryptocurrency exit scams became very popular during 2017, with the boom of initial coin offerings (ICOs). New and promising projects used their influence and community to promote upcoming coins, promising incredible returns only to later skip on the delivery process and run away with user funds.

In recent times, there are once again “exit scams” in many different forms linked with all the new developments in the crypto space:

- Decentralized finance-related projects listed on decentralized exchanges are very risky, as the space is full of “rug pulls” (another form of exit scam). It has happened several times, even with coins listed on popular centralized exchanges. One example is the recent project TITAN from Iron Finance, which attained large popularity mainly due to an investment by Mark Cuban.² After the “rug pull,” Cuban asked for improved regulation in this space,³ something inherently impossible due to the nature of decentralization.
- Nonfungible tokens (NFTs) are now literally being created by anyone with a decent following. Celebrities, YouTubers, athletes, you name it. If you check the oversaturated space right now, it may seem that NFT stands for No Freaking Talent. And yet, the art often sells for dozens of Ethers, only to be left illiquid without anyone interested in the secondary markets. One example of this is the recent sale of Logan Paul’s NFTs, which would award three buyers with a first edition pack of Pokémon cards valued at \$40,000 along with other prizes. The NFTs initially received inflated valuations of \$20,000-plus dollars but now some are left unsold at price points lower than \$1,000 on OpenSea.⁴
- Finally, another fun concept that surfaced recently was the sale of tweets. In other words, people can buy the ownership of a celebrity’s tweet by turning it into an NFT. A few days after the release, one user paid \$639 to acquire a tweet that was deleted⁵ shortly after. Talk about a genuine exit scam.

How to protect yourself from exit scams

Most investors that enter the space at this relatively mature stage will wonder how they can best spot which projects are legitimate and which are not. The following are a few tips to keep in mind when it comes to exit scams, all of which have to do with investment strategies:

- Before becoming impulsive and buying tokens that a favorite YouTuber is promoting (usually at an already inflated price), make sure to check the project’s fundamentals. Very often, the project is simply a cheaper “copy” of an already existing solution without strong foundations for its future growth.
- Do research when it comes to projects that are offering above-average returns. While some may be legitimate, others may be very risky. More specifically, make sure to learn all about staking, yield farming and high-yield savings accounts for crypto. Also, make sure to use price tracking platforms like CoinGecko regularly to get the latest information and research materials when it comes to the tokens of interest.



- If there is a project of interest along with a strong impulse to buy it, wait. Give it at least a week and observe the direction of the price. Very often, the source of influence promotes the coin at a local top, which enables interested parties to let it cool off before entering at a better position.

Above all, it is important to understand that the value of cryptocurrencies increases when one is patient. While a favorite Twitter account may be longing small-cap coins with 100 times the leverage, the chances of actually making a profit in the industry increase multifold when taking a long-term approach.

Therefore, it is also important to realize that going with the winner offers a near-certain success, despite the midterm fluctuations often seen in cryptocurrency prices.⁶ Invest in the likes of Bitcoin, Ethereum and native tokens of popular exchanges like UNI, BNB or FTT. While the price may fluctuate over the short to midterm, there is now enough evidence to reliably assume a long-term uptrend. Even if this is not the case, however, the increased liquidity of such projects enables investors to enter and exit their positions quickly. This is not possible in the NFT world, where users are often stuck with an expensive piece of art during a declining market, only to find themselves with regrets of an overpriced mistake.



Conviction, liquidity and real-world cases are still the most important factors when it comes to investing in digital assets. To avoid being scammed, it is important to live by the principle of “if it is too good to be true, it is probably a scam.” 

Judy Smith, marketing manager/writer, Paybis, Latvia, smijudy33@gmail.com

¹ “Buy Bitcoin with Credit Card or Debit Card,” *paybis*, <https://paybis.com/>

² Jeff Benson, “Mark Cuban ‘Hit’ by Apparent DeFi Rug Pull,” *Decrypt*, <https://decrypt.co/73810/mark-cuban-hit-apparent-defi-rug-pull>

³ Billy Bambrough, “Billionaire Bitcoin Investor Mark Cuban Calls For Crypto Regulation After Price Of Radical New Token Suddenly Crashes To Zero,” June 18, 2021, <https://www.forbes.com/sites/billybambrough/2021/06/18/billionaire-bitcoin-investor-mark-cuban-calls-for-crypto-regulation-after-price-of-radical-new-token-suddenly-crashes-to-zero/?sh=1361db762607>

⁴ Geoff Weiss, “Logan Paul Sells \$5 Million Worth Of NFTs Ahead Of His Pokémon Box Break,” *Tubefilter*, February 22, 2021, <https://www.tubefilter.com/2021/02/22/logan-paul-sells-5-million-nfts-pokemon-box-break/>

⁵ Jamie Redman, “NFT Immutability Debate Grows as Tokenized Tweets Get Deleted and NFT Images Are Replaced,” *Bitcoin.com*, March 11, 2021, <https://news.bitcoin.com/nft-immutability-debate-grows-as-tokenized-tweets-get-deleted-and-nft-images-are-replaced/>

⁶ “Prices,” *paybis*, <https://paybis.com/price/>

Symphony

AYASDI

**If you could have one wish today,
what would it be?**

- Holistic detection of true financial crime
- AML, Counter-Terrorism and Fraud solution
- Able to discover and stop criminals
- Less noise, more productivity

SensaAML™ :
**Next Gen Financial
Crime Discovery**



Learn more!



Data's impact on compliance and AFC operations

Threats against financial institutions (FIs) continue to rise. Add to that the pressure of ever-evolving regulatory and compliance requirements and it makes for a trying environment in which to do business. A recent report cited a 141% increase since 2019 in global fines and penalties, with FIs headquartered in the U.S. incurring \$7.5 billion in fines alone.¹ The global pandemic only served to continue exacerbating the volume, velocity and complexity of these risks, in turn driving a sharper demand for data and the informed insights necessary to protect and mitigate risk properly. But too many FIs have one arm tied behind their back, hampered by the inability to manage data properly, which can have dire consequences.

Data is, after all, the lifeblood of the financial crimes industry. Good quality data, managed in effective and efficient processes, enables FI leaders to succeed in their roles. As the world rebounds from the pandemic, the data environment has clearly changed. Two factors seem to be primarily driving these changes:

- **The regulatory focus is constantly evolving:** Domestic and international regulators are reshaping and expanding their mandates. There are expectations that new and emerging technologies should be reviewed, tested and deployed. For example, the U.S. Anti-Money Laundering Act of 2020 (AMLA) specifically addressed industry technology capability issues. Unsurprisingly, organizational response during 2020 and into 2021 waned as companies struggled to retool their technology and human assets to handle these alerts.
- **The sheer amount and diversity of data is becoming increasingly complex:** In recent years, banks and other FIs have amassed huge amounts of data on their customers and partners. Coupled with the emergence of data from the dark web, crypto and electronic communications, new challenges have emerged; this data simply cannot be layered into preexisting technologies and workflows that were not designed for these data sources and types.

An alternative to inefficiency

The reliance on virtual data ecosystems is greater than ever, but traditional data sources and the disparate legacy technology systems that analyze that data are more stressed than ever. Many FIs have adopted aggressive digital strategies, in part, to increase efficiency and create deeper relationships with their customers around the world. But these strategies significantly increased data volumes and the institutions, already overwhelmed, lacked the capacity to reconcile, interpret and act upon this information appropriately. For FIs especially, this can have a direct effect on an organization's ability to meet increased know your customer (KYC) and customer due diligence (CDD) requirements amid new regulations like the Payment Services Directive 2 in the European Union. As a result, institutions must now take additional steps to know their customer's customer. Such requirements are placing significantly greater stress on both existing technology and compliance operations.

Traditional compliance solutions rely on batch or day's old data extracted from the core banking system and other operational data sources from multiple locations. This creates significant latency in a world that is going toward real-time transacting; microsecond decision making is required to combat the many threats institutions face, inclusive of regulatory matters but extended to payment fraud, cyberattacks and more.

On top of the data processing challenge lies an even greater problem: the analytics strategy these systems use to answer existing transaction monitoring (TM) exam questions. Many of the rules emanate from known and understood illicit criminal activities identified in the 1990s with few updates since. They tend to treat all customers the same, which they are not. They rarely include or appropriately leverage risk metrics from a CDD system or other onboarding and periodic risk assessment data. These rules tend to run in a mutually exclusive manner against other rules in play. As such, they do not adequately identify holistic entity risk based on overall entity behavior.

So, what is the outcome? Tons and tons of noise that results in false positive alerts. At a false positive rate of up to 90%,² this means huge inefficiencies for investigators, massive operational costs and worse: investigators are not able to focus on identifying real and complex threats to the organization, the kind that typically generates headline news for regulatory violations. While not a new problem, most would say the level of false positives is ever increasing, causing investigators to work through larger and larger backlogs.

At the core of the problem is data pertaining to the banked customer and the need to have a clear 360-degree view of who the customer is and their valid predicated behavior. Changing alerting thresholds by dialing up or down sensitivity defeats the purpose of effectively identifying money laundering, fraud or sanctions violations. Accurately scoring what is legitimate customer behavior—based on a foundation of solid and complete data pertaining to the customer, keenly scored in the risk-rating matrix—is the only path forward to quality prevention and effective compliance. However, finding this balance requires new, dynamic approaches that are not reliant on antiquated, static data analysis of overwhelmed, disparate data collection and TM systems.

Instead, institutions must get out in front of the traditional core banking TM paradigm and alleviate the slow, antiquated batching architecture methods by utilizing real-time streaming analytics technology. Sharing information across lines of business is only heightened by the volume and diversity of types of data. When data is captured, effective technology should exist to analyze the information—in a microsecond—and to generate an alert when appropriate.

By deploying technology on the front end for analysis, the FI can then route the results to solve the various “test” questions that are being addressed. Typically, these questions need to be answered for the many lines of business that often have common constructs. By deploying results derived from real-time data analysis, reports that had historically been “locked” in a single silo technology analysis and reporting environment can now be seamlessly shared across many lines of business. With this more efficient capture and storage, the results derived from enabling and including artificial intelligence (AI), machine learning or robotic process automation (RPA) will be of greater value.

In conclusion

Clearly, the challenge now is for FIs to evaluate their present technologies and determine how and if those technologies can be modernized and adjusted to address the massive data onslaught

and the ever-changing threat environment. The following steps can help provide a benchmark for better business management and risk protection:

1. Perform an audit of existing processing and practices to identify the root causes of problems, including what and how data is received, to determine the impact that data quality and content has on end results. This audit may be conducted by a third-party consultancy in concert with technology providers.
2. Obtain opinions and insight from internal team members to reveal shortfalls of existing technology and then begin a project for updating, replacing or augmenting those technologies.
3. Closely review existing regulatory mandates that are focused on lines of business requirements to determine immediate needs that must be addressed to avoid penalty or mandated correction. Consider alternative technology that will mitigate this risk by improving processing and assisting human assets to perform their tasks with greater efficiency.
4. Invest in streaming analytics that can be deployed in front of the core banking system, and natively in the payments processing channel for a proactive response to risk, instead of the existing reactive “the deed is done already” approach.
5. Employ advanced analytics for anomaly detection to shine a light on risks that are unidentifiable by existing rules and discover never-before-seen risk that could lead to fines.
6. Augment existing TM systems for “entity level” 360-degree behavioral risk analysis post-alert generation to cut the noise, prevent false negatives, and add efficiencies through RPA at the level 1 “triage” and level 2 “disposition” steps. This ultimately cuts costs, identifies real risks and keeps institutions in good standing with regulators—culminating in fine avoidance, loss of shareholder value and reputational damage.

Every day, FIs must combat attempts to compromise their technology infrastructure. Ransomware attacks and demands have affected operations and response methods across FIs, corporations and government entities. In the U.S. and other countries, the evolution of domestic terrorists has changed the responsibility of FIs to identify individuals and their assets, which may be present in customers’ accounts and associated behaviors.

Have you optimized your technology and compliance approach to prepare for this new reality? 

John Dalton, SVP, global head of financial services product and solutions strategy, KX

Robert Goldfinger, CAMS, capt. (ret.), head of fin crime technology sales, KX

¹ Jaclyn Jaegar, “Report: Fines against financial institutions hit \$10.4B in 2020,” *Compliance Week*, December 22, 2020, <https://www.complianceweek.com/surveys-and-benchmarking/report-fines-against-financial-institutions-hit-104b-in-2020/29869.article>

² Stuart Breslow et. al, “The new frontier in anti-money laundering,” *McKinsey*, November 7, 2017, <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-new-frontier-in-anti-money-laundering>



***The nexus between
Ransomware, Cryptocurrency
and money laundering***



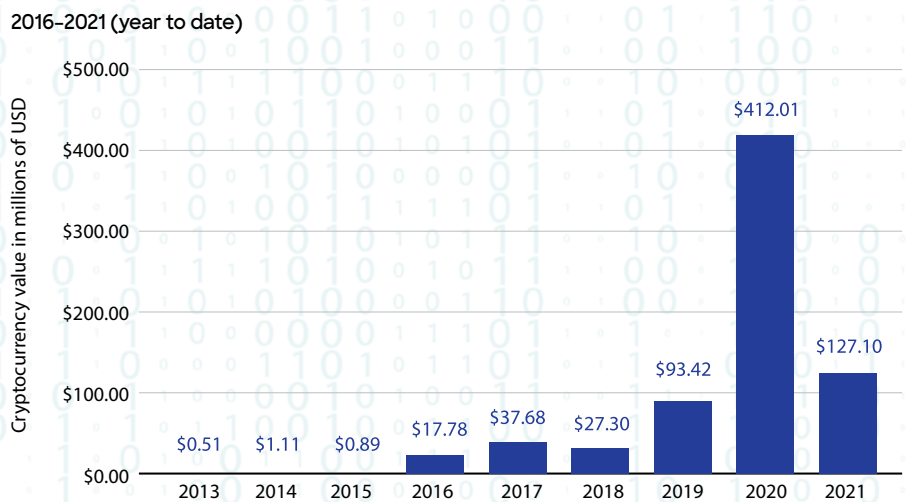
In May 2021, American motorists across the states of Virginia, Georgia and North Carolina panicked as they scrambled to fill their vehicles at gas stations. The run for fuel was a result of a cyberattack on the Colonial Pipeline, which was forced to shut down its supplies of diesel, petrol and jet. Colonial Pipeline's operations were disrupted by a ransomware attack perpetrated by Darkside—a criminal gang that demanded a ransom of 75 bitcoin (\$4.3 million). After Colonial Pipeline made the crypto payment, it received a decryption tool to unlock the systems compromised by the hackers.¹ In another case on July 3, 500 supermarkets of Coop Sweden were forced to shut down as their point-of-sale tills and self-service checkouts stopped working. The chain itself was not targeted by hackers, but it suffered from the contagion effect when one of its software providers was the victim of a ransomware attack. The provider warned all its customers to stop using its service immediately and go offline.²

The FBI Cyber Crimes Squad clawed back 63.7 bitcoin (\$2.3 million) paid by Colonial by tracking the ransom to a cryptocurrency address.³ But the Colonial Pipeline has not been the only victim. Other institutions that have fallen prey to ransomware criminals—such as Ryuk/Conti, Sodin/REvil, ClOp, DoppelPaymer, DarkSide and Avaddon—include Canadian aircraft manufacturer Bombardier, the Washington D.C. Police Department, electronics company Acer, the University of Colorado, the cities of Atlanta and Baltimore, Quanta Computer and the CNA Financial Corporation. Much of the extortion has been in the form of cryptocurrency—also known as convertible virtual currency (CVC). It is a digital representation of value that is a medium of exchange, a unit of account, and/or a store of value. Cryptocurrency is not issued or regulated by any entity. Those who deal in CVC do so at their own risk and accept the wild variances of the exchange rate.

The allure of cryptocurrency for ransomware

In 2020, over \$400 million in cryptocurrency remitted to digital addresses was linked to ransomware criminals, a concerning trend for law enforcement, financial institutions (FIs), insurers and other stakeholders (see Figure 1).

Figure 1: Total cryptocurrency value received by ransomware addresses



Source: "Ransomware 2021: Critical Mid-Year Update," Chainalysis, May 2021, <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>

So, what can explain criminals' attraction to cryptocurrency and why is it so popular? The term "crypto" is derived from the Greek word *kryptós*, meaning "hidden." In today's parlance, cryptocurrency is used to refer to alternate payment mechanisms like Bitcoin, Ethereum, Litecoin, Zcash and the lesser known Monero, which prides itself on being "secure, private and untraceable" based on a Google search. Hackers like the anonymity and opaqueness of the cryptographic techniques that safeguard digital addresses and mask the destination of funds. They infect victims' computers with malicious software by running email phishing campaigns, exploiting remote desktop protocol vulnerabilities and identifying security weaknesses in widely used software programs. The malware encrypts data on a company's computers, thereby making it unusable. The cybercriminals hold the company hostage by threatening to destroy victims' data or publishing it on social media until they receive the ransom. Only then is the information decrypted and access restored to systems or data. The impact of ransomware on the operations of the state, government institutions, police and fire departments, hospitals, airlines and other critical infrastructure cannot be underestimated.

The three stages of cryptocurrency-based money laundering

The nexus between ransomware and money laundering is established when a CVC is used as the medium of exchange. Figure 2 illustrates the three stages of CVC money laundering. This growing trend resulted in the Financial Crimes Enforcement Network (FinCEN) issuing an advisory in October 2020.⁴ According to FinCEN, “Processing ransomware payments is typically a multi-step process that involves at least one depository institution and one or more money services business (MSB).” As most victims do not hold cryptocurrency wallets or accounts, the delivery of a ransom entails funds transmitted from their bank accounts at regulated FIs to a CVC exchange. This is the placement stage. There have also been instances where digital forensics and incident response companies or cyber insurance companies receive the victim’s funds, exchange them for CVC and then transfer the CVC to designated digital addresses that are under the control of the cybercriminals.

Another methodology involves scammers soliciting people to accept a “donation” of funds into their own bank account in lieu of a fee. They are given instructions to convert the funds into a CVC and remit it further to different digital addresses. The “donation” is most likely ransom money or money stolen from others. In a world during a pandemic, there are enough willing money mules who have no compunctions in allowing their bank accounts or digital addresses to be used for nefarious purposes.

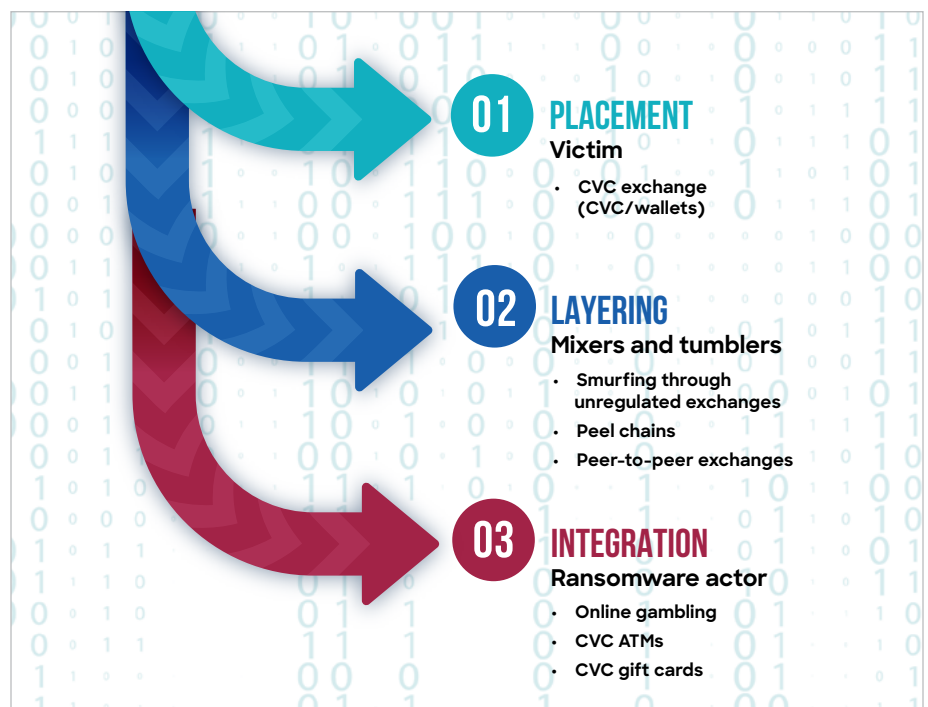
The layering stage commences when the gangsters mix the ransom received with other cryptocurrency funds by pooling together multiple funds from a chain of digital addresses during a random period. This is done to obscure the CVC trail and break the connection between an address sending a CVC and the addresses receiving the CVC. Mixers and tumblers like AlphaBay, Helix, Darklaunder, Bitlaunder and CoinMixer accept the cryptocurrency, mix the funds received

from different sources and then remit it back to another series of destination addresses in lieu of a 1% to 2% fee. According to Chainalysis,⁵ the time taken for mixing could range from a short period of one to six hours, to a longer one of up to seven days depending on the complexity of the transaction. Once a transaction has gone through a mixing service, the prior addresses associated with the coins are effectively erased.⁶

Other methods of layering involve smurfing cryptocurrency transactions across many accounts and exchanges or moving the CVC to unregulated exchanges or peer-to-peer exchanges in jurisdictions known for having weak anti-money laundering/counter-terrorist financing (AML/CTF) controls. This technique involves the use of peel chains, which are chains of wallets that funds pass through to hide their trail of illicitly obtained CVC.

The last stage of cryptocurrency-based money laundering is integration, which is when the ransom is legalized to demonstrate that it belongs legally to the cybercriminal. Conduits that facilitate the cleaning of digital assets include unregulated cryptocurrency exchanges that do not require identity checks of its users and have lax security policies. They facilitate the conversion of CVC into fiat currency. Other mediums of exchange are the online gaming and gambling sites that accept payments through CVC, which can be used to purchase credit or virtual chips. These sites are patronized by criminals who convert them into legal currency through a series of small transactions. CVC ATMs and CVC gift cards are another source of exchange. According to coinatmradar.com, there were approximately 23,000 crypto ATMs across the world in early July.⁷ This is not a huge number but it is enough to support money laundering. There is also the trend of consumers using cryptocurrencies to buy luxury goods. Upscale watch manufacturer Franck Muller launched a \$12,000 watch earlier this year that functions as a timepiece as well as a digital wallet. Available for purchase solely through bitcoin, the watch has its own unique public address etched on the 41 mm dial and a sealed USB containing the private key.⁸

Figure 2: Three stages of CVC money laundering




THE LOOMING RISK TO FIs, REGULATED CVC EXCHANGES, CYBER INSURERS AND ENFORCEMENT AUTHORITIES IS THAT THERE IS LITTLE KNOWLEDGE OF THE IDENTITY OF THE RECIPIENT IN CONTROL OF THE CVC FUNDS

Conclusion

Cryptocurrency is an ideal option for those trying to avoid strict capital controls, launder illicit gains or evade financial sanctions on countries, corporations, individuals or terrorist organizations. The looming risk to FIs, regulated CVC exchanges, cyber insurers and enforcement authorities is that there is little knowledge of the identity of the recipient in control of the CVC funds. What if the payments are made to addresses belonging to sanctioned individuals or addresses connected to ransomware strains associated with cybercriminals based in heavily sanctioned jurisdictions? OFAC has already linked two digital currency addresses to the sanctioned perpetrators of the SamSam ransomware attacks that targeted corporations, hospitals and universities. These wallet addresses formed part of the layering phase of money laundering as they were used to transact with over 40 different digital currency exchanges across the world.⁹

Unfortunately, the digital currency address listings are not exhaustive or all-comprehensive. It is even worse when stealth addresses are used. This occurs when the sender uses a one-time address for each transaction. Multiple transactions done by the same sender for the same recipient have different addresses, thereby obscuring the details of the CVC payments and their financial details. Institutions that engage or facilitate transactions to digital addresses hence run the risk of fines and/or losing access to their dollar-clearing facilities if it transpires that the funds made their way to sanctioned individuals or entities.

Although several regulators have demanded full transparency and disclosure of the beneficiary and the remitter's addresses as well as the purpose of fiat currency-based fund transfers, they have not restricted the holding and trading of virtual currency in their jurisdictions. There are varying levels of control—certain countries have banned FIs and payment companies from providing services related to cryptocurrency transactions but have not outlawed their citizens from holding CVCs. Others have left it to the discretion of FIs—many of whom have made it explicit to their customers that their bank accounts cannot be used for cryptocurrency transactions.

The recent Carbis Bay G7 Summit Communiqué emphasized the need for governments to “identify, disrupt and hold to account those within its borders who conduct ransomware attacks, abuse virtual currency to launder ransoms, and other cybercrimes.”¹⁰ But until greater concerted cross-border efforts are made, institutions must be proactive in terms of implementing cybersecurity controls, conducting regular business continuity simulations and promoting cyber hygiene practices¹¹ as it is always better to be safe than sorry. 

Deepa Chandrasekhar, senior vice president, chief compliance officer, MLRO, United Gulf Bank B.S.C. (c)

The views expressed in this article are the author's alone and do not represent those of the organization.

¹ Thomas Brewster, The Ransomware Group Behind The Colonial Pipeline Hack Says It Is Disbanding,” *Forbes*, May 14, 2021, <https://www.forbes.com/sites/thomasbrewster/2021/05/14/the-ransomware-group-behind-the-colonial-pipeline-hack-says-it-is-disbanding/?sh=14e242eb7775>; Nicole Perloth, “Colonial Pipeline Paid

75 Bitcoin, or roughly \$5 million, to hackers,” *The New York Times*, May 13, 2021, <https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html>

² Joe Tidy, “Swedish Coop supermarkets shut due to US ransomware cyber-attack,” *BBC*, July 3, 2021, <https://www.bbc.com/news/technology-57707530>

³ Matthew J. Schwartz, “How Did FBI Recover Colonial Pipeline’s DarkSide Bitcoins?” *BankInfoSecurity*, June 11, 2021, <https://www.bankinfosecurity.com/how-did-fbi-recover-colonial-pipelines-darkside-bitcoins-a-16863>

⁴ “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” *Financial Crimes Enforcement Network*, October 1, 2020, <https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>

⁵ Thibault de Balthazar and Julio Hernandez-Castro, “An Analysis of Bitcoin Laundry Services,” *Chainalysis and University of Kent*, September 2017, https://www.researchgate.net/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services (accessed June 28, 2021).

⁶ Faisal Khan, “Twitter hackers employing ‘peel chains’ to launder the Bitcoin bounty,” *Technology.org*, July 23, 2020, <https://www.technology.org/2020/07/23/twitter-hackers-employing-peel-chains-to-launder-the-bitcoin-bounty/> (accessed June 28, 2021).

⁷ *Coin ATM Radar*, <https://coinatmradar.com/> (accessed July 8, 2021).

⁸ Rachel Cormack, “Franck Muller’s Newest Watch Doubles as a Bitcoin Wallet, and You’ll Need Cryptocurrency to Buy It,” *Robb Report*, February 24, 2021, <https://robbreport.com/style/watch-collector/franck-muller-new-timepiece-doubles-bitcoin-wallet-1234598536> (accessed June 30, 2021).

⁹ “Treasury Identifies Iranian Nationals and Their Digital Currency Addresses Used to Facilitate Ransomware Attacks,” *JD Supra*, December 4, 2018, <https://www.jdsupra.com/legalnews/treasury-identifies-iranian-nationals-29943/>

¹⁰ “Carbis Bay G7 Summit Communiqué,” *The White House*, June 13, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communication/>

¹¹ “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” *Financial Crimes Enforcement Network*, October 1, 2020, <https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>



Casinos and the why of money laundering

Casino employee observations are a critical component of a casino anti-money laundering (AML) program because, unlike banks, almost all transactions of a casino customer occur while the patron is on the business premises. Accordingly, a casino should emphasize AML training that strives to enhance the ability of casino employees to identify unusual behavior worthy of a suspicious activity report (SAR).

The general consensus of learning experts is that training should be emphasized on understanding rather than merely memorizing the curriculum. Too often, AML training for casino employees focuses on memorizing typologies of suspicious transactional behavior (the how) without explaining why a money launderer would engage in such transactions.

Money laundering is not a lofty subject that only seasoned AML professionals can understand. Hit TV shows like *Ozark*, *Narcos* and *Breaking Bad* do a relatively good job of getting the public to make sense of money laundering. Their scripts are heavily peppered with dramatizing the why of money laundering—the why is what makes the shows engaging and entertaining.

One of the most-watched TED Talks (over 55 million views) is by famed organizational expert Simon Sinek regaling the benefits of explaining the why. In Sinek's best-selling book, *Start with Why: How Great Leaders Inspire Everyone to Take Action*, he asserts that successful organizations inspire their employees by putting the why (the purpose) before the how (the process). When it comes to AML training and casino risk assessments, casinos should follow the lead of Sinek and start with the why.¹

In a broad sense, the why for criminals to launder their money is to stay off law enforcement’s radar so that their money trails do not incriminate them. This is the overarching goal of money laundering, but it does not explain why they engage in certain transactions (or processes) to accomplish their ultimate money laundering goal. The ultimate goal of a doctor is to heal their patients but this does not explain why they engage in certain processes, such as listening to a patient’s heart, drawing blood or taking an x-ray. Each procedure a doctor conducts is intended to accomplish a specific goal. When a patient understands why their doctor conducts certain processes, they are in a much better position to make sense of their treatment and gauge whether certain procedures are necessary.

When casino employees understand why money launderers engage in certain processes, they are better positioned to diagnose whether transactions are suspicious or simply expected gaming behavior.

Money laundering goal methodology

An intuitive approach to teaching the why behind money laundering transactions is the money laundering goal methodology (MLGM). This methodology focuses on the intent of the transaction and explains money laundering using relatable terms. When a criminal engages in a specific money laundering transaction, they set out to accomplish at least one of the money laundering goals described in Table 1.

Using the MLGM training approach allows casino personnel to make sense of money laundering transactions. Why would a criminal structure cash deposits, use a false ID, play as an unknown, switch seats or use a nominee to conduct a transaction on their behalf? Because the criminal may intend to conceal their activities from authorities. And why would a criminal stuff a slot machine with small bills and then cash out, make numerous debit card cash withdrawals or regularly cash checks? Because the criminal may intend to convert their funds so they are not as traceable or so they are more convenient to use.

Table 1: Casino money laundering goals and intents of transaction

Casino money laundering goal	Intent of transaction
Conceal	To hide the beneficial owner’s identity from a transaction or information report filed with the government
Convert	To convert funds to a form that is less traceable and/or more convenient to use
Transfer	To transfer funds from one person or place to another
Clean	To create an alibi that funds originated from gaming winnings or to obfuscate the money trail
Spend	To enjoy illicit funds often without regard to accomplishing any other money laundering goal
Store	To store funds outside the traditional banking system





MLGM-based training positions casino personnel to think like a money launderer by focusing on the why. In addition to increasing the ability to retain AML training material, the MLGM puts casino personnel in a better position to isolate transactional behavior emblematic of money laundering and diminishes their risk of falsely identifying transactions that are not indicative of money laundering. If a transaction does not appear to accomplish a money laundering goal, it may not be indicative of money laundering.

Identifying money laundering goals and processes

It is important to differentiate the money laundering goal from the process used to accomplish the goal. Leaving significant funds in a dormant front money account, holding on to a large casino check rather

than depositing it and hoarding casino chips are not money laundering goals but processes to accomplish the goal of storing funds. Acquiring W-2G forms, commingling illicit funds with gambling winnings or attempting to obtain a cash withdrawal receipt from the cage are also not money laundering goals but instead processes to accomplish the goal of cleaning funds.

The processes used to accomplish a money laundering goal are the how, not the why. Teaching the how (the processes) without explaining the why diminishes the ability of casino personnel to retain and make sense of the curriculum. Conversely, by first teaching the why then providing examples of the how, casino personnel are better positioned to make sense of money laundering. They can determine if a specific transactional pattern indicates money laundering or if it is just a patron's unique gaming style. For instance, someone may not want to redeem over \$10,000 in chips at one time because they want to return to the casino soon. Their goal is to gamble again without having to buy chips rather than the money laundering goal to conceal.

The best way to determine the why of the transaction is to look at the person conducting the transaction. In particular, what is known about their source of funds and history of gambling? If it is determined that the patron's funds are derived from legitimate sources, why would they need to accomplish a money laundering goal? Trying to determine the why solely based on transactional information may result in falsely classifying transactional activity as suspicious. The MLGM drives casino personnel to focus on the who of the transaction in determining the why of the transaction.

Criminal investigators building money laundering cases need to prove the intent of the transactions in question. There is no criminal case if evidence does not show the intent to launder money. Just because someone places funds into a slot machine and then cashes out with little or no play (a pattern known as minimal play) does not mean they intended to commit money laundering. Compliance personnel trained in the MLGM will be more adroit in analyzing transactional behavior, such as minimal play, to root out whether there appears to be an intent to accomplish a money laundering goal, whether the patron is merely engaging in a particular style to gamble or whether they are funding their gaming. Moreover, by doing so, they are more skilled in crafting SARs to include information that is useful to law enforcement (the who, the how and the why).

The MLGM also helps compliance personnel understand why certain controls are required to detect, prevent and report money laundering. When casino personnel make sense of the controls, they will be more willing to ensure these controls are followed.

Table 2 on the right is a breakdown of the money laundering goals and the known processes to accomplish these goals.

Tax evasion and terrorist financing

Generally, in order to prosecute the charge of money laundering, the transaction has to involve illegal proceeds. This is why due diligence concerning the source of funds is critical to an effective AML program because most of the time criminals simply just spend their dirty money at casinos. On the other hand, most of the time tax evasion involves legitimate funds, but tax evaders may need to accomplish certain money laundering goals, such as concealing, converting, transferring and storing funds. Their ability to accomplish such goals is rather limited at a casino compared to other financial institutions. As the "2018 U.S. Treasury National Money Laundering Risk Assessment" demonstrates, casinos are not known for facilitating tax evasion schemes but under the Bank Secrecy Act (BSA), casinos are required to report suspicious activity involving tax evasion.²

Funding terrorism does not always involve illegal processes, but terrorist financiers may use a casino to accomplish certain money laundering goals to further their criminal activity, such as converting, transferring, hiding or storing funds. However, the "2018 U.S. Treasury National Terrorist Financing Risk Assessment" makes no mention of casinos.³

Table 2: Casino money laundering goals and processes

Casino money laundering goal	The processes
Hide	<ul style="list-style-type: none"> • Structuring • False ID • Nominee • Chip walk • Seat switching • Unrated play
Convert	<ul style="list-style-type: none"> • Small to large bills • Cash-out of a debit card • Check cashing • Cash-to-gaming instrument
Transfer	<ul style="list-style-type: none"> • Paying others' markers/expenses • Using chips as a form of currency • Third-party payments
Clean	<ul style="list-style-type: none"> • Acquiring W-2G forms • Commingling/layering • Offset betting • Obtaining withdrawal receipts
Spend	<ul style="list-style-type: none"> • Gambling losses • Retail items • Entertainment • Food and beverage
Store	<ul style="list-style-type: none"> • Dormant front money • Hoarding chips • Casino check was not deposited • Funds stored on gaming wallet

Sports wagering and facilitation

If a casino offers sports wagering, it may be appropriate to add another money laundering goal: promote. To promote is to use the casino to continue facilitating criminal activities. In the case of sports wagering, illegal bookmakers are known to use the sportsbooks to balance their books so they are not lopsided on any one game outcome, a process commonly referred to as laying off bets.

The other important why

Not only should casino personnel understand the why for money laundering transactions, they should also be trained in why Bank Secrecy Act/anti-money laundering (BSA/AML) efforts are essential in preventing criminals from using casinos to facilitate their criminal activity. By doing so, they will understand that the BSA is an indispensable tool for law enforcement and that casino currency transaction reports (CTRs) and SARs have played an important role in bringing to justice a wide variety of significant criminals, including drug dealers, human traffickers and major fraudsters. They will see that their efforts help keep their community safe. Understanding the why of BSA/AML will inspire casino personnel to participate in the AML process.

Placement, layering and integration: The PLI model

Traditionally, BSA/AML professionals explain the why of money laundering by breaking down the process into the three stages of placement, layering and integration, commonly referred to as the PLI model. Although the PLI model works to explain the why of sophisticated


Table 3: PLI model and casino money laundering goals

PLI model	Casino money laundering goal
Placement	Conceal
	Convert
	Transfer
Layering	Clean
Integration	Spend
	Store

money laundering in large-scale money laundering operations, such as those of cartels, it does not translate well to casino money laundering. Often, when patrons bring illicit funds to a casino, they do it without regard to completing the three stages of the PLI model. For instance, many criminals only need to avoid having a CTR filed on them to stay off law enforcement’s radar. Why explain money laundering as a three-stage process when many criminals only intend to engage in a single transaction to complete their money laundering? Another consideration is that illicit funds more commonly enter a casino simply for enjoying the fruits of a crime without any past or present conscious effort to complete a money laundering cycle.

The MLGM places emphasis on the why of the individual transaction without regard to forcing the transaction into one part of a money laundering cycle. That said, MLGM does reconcile with the PLI model cycle as shown in Table 3 above.

Conclusion

To catch a money launderer, one must think like a money launderer. When starting with the why, casino personnel put themselves into the head of a criminal trying to stay off law enforcement’s radar. The why allows casino employees to make sense of the money laundering or, and just as important, to understand why the transactions are merely the results of a patron’s gaming style. The why allows the AML program to be more risk-based and reduces the chance of reporting transactions to the government that are, in reality, legitimate patrons simply enjoying the casino. In this respect, the AML program becomes more useful to law enforcement as they combat financial crime. 

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

¹ Simon Sinek, “How great leaders inspire action,” filmed 2009, TED video, 17:27, https://www.ted.com/talks/simon_sinek_how_great_leaders_inspire_action?language=en

² “2018 National Money Laundering Risk Assessment,” U.S. Department of the Treasury, https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf

³ “2018 National Terrorist Financing Risk Assessment,” U.S. Department of the Treasury, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf



Don't let the
criminals win.

Move from
defensive to
offensive AML
with **advanced
analytics.**

Increase your program
effectiveness with
NICE Actimize solutions.
Trusted, Proven, Always
Innovating

Less than 1% of the estimated USD \$4 trillion laundered by criminals every year is recovered. It's no secret that we need to be more effective – we cannot continue down the same path and expect different results. Only when we understand our customers better can we effectively manage risk to better spot the criminals.

NICE Actimize is the market leader in AML solutions. We provide the tools you need to understand your customers from the start of their relationship to the very end. Know your customers contextually by injecting both internal and external data across their lifecycle, all while infusing your solutions with AI and machine learning to help you identify normal vs. abnormal behavior.

**Understand your customer, understand
their risk, fight financial crime.**

Get Started



Strengthening your DPMS toolkit



The dealers of precious metals and stones (DPMS) sector as well as the commodities traded within it, are often poorly understood by financial institutions (FIs). This is a sector that is unique from other anti-money laundering (AML) regulated reporting entities because the industry is purely built on retail sales to the consumer, and the commodities traded internationally throughout the industry are controlled differently depending on the laws in each country. In addition, the commodities involved (i.e., diamonds, gemstones and precious metals) are not only used to store and transfer wealth, they are also used as an alternate currency and for generating proceeds of crime. The jewelry industry itself is unaware of much of the money laundering that occurs. In addition, the proceeds from both legitimate and illegitimate activities flow into the jewelry industry and then into the banks that service them. Collectively, these factors compound and create elevated DPMS AML risk exposure.

Money laundering via precious metals and stones

One of the most common misconceptions is that money laundering simply involves the acquisition of other goods using cash obtained from illegal activities. While the premise is true, it misses an entire segment of money laundering that involves the disposal of goods obtained illicitly for cash or other goods (in trade). This concept is particularly important to jewelry crimes relating to the theft and other criminal acquisition of diamonds, gemstones and precious metals. The disposal, or laundering, of the jewelry occurs when it is traded for drugs or other goods, or when it is sold back to the legitimate market. When a jeweler conceives that money laundering is about the sale of jewelry to a criminal for cash, they miss the laundering activity by a criminal who sells them illicit jewelry.

This is particularly important given the propensity of the loss of jewelry due to theft, robbery, or breaking and entering. Consider that jewelry is often the second item that is most often stolen in a residential breaking and entering.¹ Also, consider that the average loss in these events is approximately \$2,566.² Given the FBI statistics that there are 376 residential incidences of breaking and entering per 100,000 population³ (in 2018, 431 per 100,000 in Canada⁴) one can estimate that jewelry loss to this crime is as high as \$20,000,000 per year in a city of 5 million people in the U.S. This jewelry is eventually laundered back into the legitimate jewelry market and these proceeds ultimately

flow into the banks that service the industry. This is simply one possibility of laundering that can occur through the DPMS sector. The actual purchase of new jewelry, such as high-end watches and heavy high carat gold and diamond jewelry by criminals using proceeds of crime, is another possibility as well as the use of diamonds and gemstones in trade-based money laundering (TBML).

Part of the difficulty in understanding the industry is the significant variance in business models that occurs among the retailers and wholesalers. Low-end jewelry, high-end jewelry, watches, colored gemstones, diamonds, high carat gold, consignment and secondhand sales can all be the main focus of a retailer in different business models, be it a brick-and-mortar store, online or hybrid. Each have their own target markets (clients), supply chains, price points and business cycles. Depending on the business, the supply chain can be equally varied from local to national or it can be international in scope. On the supplier end, the significance is in understanding the market, suppliers and geographic location of supply.

Compounding the AML complexity is the variation in AML laws across the various jurisdictions where retail and wholesale trade are conducted. Consider the simple trade between Canada and the U.S. and the gemstones that are specifically included as “precious stones” under the respective AML laws in each country. Across these close trading partners, the difference in what precious stones are named, or not named, by their respective AML laws is significant (see Table 1 below).

Table 1: Precious stones as defined by Canada and the U.S.

Canada	U.S.
Diamond, sapphire, ruby, emerald, tanzanite and alexandrite ⁵	Diamond, corundum (including rubies and sapphires), beryl (including emeralds and aquamarines), chrysoberyl, spinel, topaz, zircon, tourmaline, garnet, crystalline and cryptocrystalline quartz, olivine peridot, tanzanite, jadeite jade, nephrite jade, spodumene, feldspar, turquoise, lapis lazuli and opal ⁶

This is just one aspect of AML legislation; variations also occur from country to country in other segments of DPMS-related AML laws. While any gemstone can be used for money laundering, colored gemstones (nondiamond) are tremendous vessels for TBML due to the lack of any internationally recognized pricing scheme. This adds additional complexity in mapping out the risk related to gemstone sourcing across various jurisdictions and for hundreds of gemstones that are not covered by AML laws. The Harmonized System—which is a system of product codes used and accepted globally for the international import and export of any product including all gemstones—has potential to capture every gemstone, but it has not been applied to laws relating to AML and gemstones.

One of the most common misconceptions is that money laundering simply involves the acquisition of other goods using cash obtained from illegal activities

A detailed knowledge of the jewelry industry is critical to understanding the DPMS business, and its market, both nationally as well as internationally

Strengthening the DPMS segment of AML compliance

Knowing where the exploit opportunity exists for criminals and where money laundering is occurring requires an understanding of the business, market and criminal use of these commodities. This is the case with the DPMS sector and the same holds true for any other reporting entity be it casinos, real estate or money services businesses. Banks can strengthen the DPMS segment of their AML compliance and risk manage accounts by enhancing DPMS sector knowledge, business model mapping and transaction analysis capabilities.


The DPMS sector is a relatively obscure market and while it has been part of the retail sector for a millennium, it is poorly understood by anyone but those who work in the business—this includes banks. A suite of tools specifically focused on evaluating DPMS transactions can elevate investigator and analysis transaction monitoring capabilities. First of all, a detailed knowledge of the jewelry industry is critical to understanding the DPMS business, and its market, both nationally as well as internationally. Equally important is knowing how criminals utilize diamonds, gemstones, precious metals and how criminal enterprises are woven into the legitimate jewelry market. Collectively this provides a comprehensive understanding of the exploitative opportunities afforded by the industry and the commodities involved and elevated points of risk.

Second, utilizing the foundational industry and business knowledge, a review of existing high-risk DPMS should be conducted by investigators experienced in DPMS account review. This would optimally include transaction reconciliation against the business model, business size, geographical region, annual sales cycle, comparative analysis to market and more. Like subject-matter experts focused on other reporting entities, investigators who have done analysis with the DPMS industry and have the business knowledge should be encouraged to become DPMS sector specialists.

Third, as both a comprehensive know your customer and preventative measure, a DPMS-specific onboarding screening should be conducted for pre-account generation. The DPMS sector is unique and businesses should have specific industry insurance, registrations, associations and business model types to name a few. And, of course, the retail DPMS requires an AML compliance program. It needs to be reviewed, registered and currently meeting the compliance requirements. The details of the onboarding questionnaire are critical as the collection of this data is used to map out the business model completely, which in turn allows comparative transaction analysis as discussed earlier.

Conclusion

The jewelry industry is a fantastic industry with a long and rich history as an integral segment of commerce across the globe. However, the nature of the industry and its many business models, along with the commodities that are bought and sold within it, afford opportunities for criminals to launder proceeds of crime. Points within the jewelry sector allow criminals to

launder proceeds of crime into the industry, which in turn funnel into the FIs that service them. While the jewelry industry is on the front line, it is not nearly as knowledgeable of money laundering, well-equipped or resourced to meet the regulatory demands as banks. On the other hand, banks, AML investigators and analysts are highly sensitive to transaction analysis related to most reporting entities. However, training, investigative/analytical guidance and specialization, as well as onboarding screening can be helpful tools to strengthening the DPMS segment of regulatory compliance. 

Kelly Ross, M.A., CAMS, FCGmA, gemologist and specialist, Kelly Ross Consulting Alberta, Canada, Kross5c@gmail.com

- ¹ Joseph B. Kuhns et. al, "Understanding Decisions to Burglarize from the Offenders Perspective," *University of North Carolina at Charlotte Department of Criminal Justice & Criminology*, December 2012, https://www.researchgate.net/publication/268444817_Understanding_Decisions_to_Burglarize_from_the_Offender's_Perspective/link/546b48410cf2f5eb18091770/download
- ² "2018 Crime in the United States," *FBI*, [https://ucr.fbi.gov/crime-in-the-u.s.-2018/topic-pages/tables/table-23](https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/tables/table-23); "Crime in the United States by Volume and Rate per 100,000 Inhabitants, 1999-2018," *Uniform Crime Reporting (UCR) Program — FBI*, <https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/tables/table-1>
- ³ *Ibid.*
- ⁴ "Table 1: Police-reported crime for selected offences, Canada, 2017 and 2018," *Statistics Canada*, <https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00013/tbl/tbl01-eng.htm>
- ⁵ "Dealers in precious metals and precious stones," *Financial Transactions and Reports Analysis Centre of Canada*, <https://www.fintrac-canafe.gc.ca/re-ed/dpms-eng>
- ⁶ "Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels," *Financial Crimes Enforcement Network*, February 21, 2003, <https://www.fincen.gov/sites/default/files/shared/antimoneylaundering060305.pdf>

A white line-art illustration of a global skyline, featuring recognizable landmarks such as the Statue of Liberty, the CN Tower, the Leaning Tower of Pisa, and the Guggenheim Museum Bilbao, set against a dark blue background.

25 ACAMS EVENTS TAKE PLACE GLOBALLY EVERY YEAR.

Covering the key issues that matter to you; from AML culture within organisations, to how technology is changing in the field, and the evolving future needs of the profession.

There's only ONE place to be.

Find out what's happening in your area:





A guide to surviving an audit



For compliance professionals, there is an addition to the adage that the only things in life that are certain are death and taxes—make that death, taxes and audits. As with death and taxes, the audit experience can be wildly divergent based on many factors, such as your industry sector, auditing bodies and personnel, your organization's risk factors and your compliance program. While a compliance professional may have little influence with external audit factors, the internal audit process can often be improved or enhanced to help make the experience less taxing and traumatic. What follows is a review of strategic audit preparation, participation and response actions that will likely make the audit process smoother.

No one likes surprises. That is why knowing your compliance requirements, your risk factors and assessment, as well as the detailed workings of your compliance program (inside and out) is critical to audit success. The audit process is designed to find gaps in your policies and procedures so that you can improve your program. With some auditors this is a welcomed activity that will help keep the regulators at bay. With others, it often seems like an adversarial relationship where it feels as though the auditors' only goal is to find fault with your program, whether that assessment is deserved or not. The goal is to eliminate or significantly mitigate potential conflict in the audit process. The keys to this are honest self-assessment of your program, acute awareness of your compliance environment, complete and comprehensive documentation as well as data management.

Obviously, the larger the organization, the more complex its compliance responsibilities. If you look at regulatory actions, many are brought about not because of willful malfeasance but because there is a lack of comprehensive command and control of compliance risks. That is why good communication and institutional knowledge not only smooth the audit process, they also help eliminate the potential of regulatory consequences, thus improving a company's reputation, legacy and—most important to senior management—its bottom line.

Audit survival begins long before the audit commences. Preparing for an audit is a constant process that should be continually assessed and honed. That is why conducting objective internal reviews and/or engaging a disinterested third-party auditor is so important. It is also important to conduct these introspective assessments regularly because the business environment and regulatory requirements are not static. What was an airtight program a few years ago could have significant issues simply because external factors have changed dramatically. Be aware of these factors before an auditor identifies them.

The following is a basic checklist of activities that will enhance your audit experience.

Audit survival checklist

Audit preparation

- Know your program inside and out and ensure that your co-workers and staff are well versed in their areas of responsibility. Discovering that some employees do not fully understand the work they are doing is a common audit finding.
- Ensure that your co-workers are fully and adequately trained. Be able to provide proof of this training. Also, be able to prove that your staff has the background and ability to perform their assigned tasks. Resumes of staff and key contractors should be current and available.
- Ensure that everyone in your organization who will interact or provide written information to the auditors is on the same page and confines their audit responses to their area of expertise. For example, an IT technician should not be offering opinions on red flags except for how those red flags are programmed into the compliance technology. Any erroneous response can come back to haunt you, even years later.
- Impress upon those interacting with the auditors that it is important to respond directly to the auditors'

questions and not go beyond the scope of the question in any response. Doing so could cause confusion and open an unexpected path of inquiry, thereby complicating and extending the audit process. Provide facts, not opinions.

- Conduct regular risk assessments and internal reviews or conduct them whenever new factors appear like new products, services or sales channels. If possible, engage a disinterested third-party auditor with a thorough knowledge of your industry to do a deep dive into your program. Auditors will likely ask for copies of these reviews and your actions to address the findings. Be prepared to provide these documents.
- Ensure your policies and procedures manuals are complete and up to date. Most importantly, be well prepared to prove that you stringently enforce your policies and follow your procedures. Auditors have little sympathy for these all-too-common deficiencies. Your organization developed the policies and procedures, so not following them as written is a common cause of regulatory penalties.
- Perform a comprehensive gap analysis and heed its findings. Ignoring or marginalizing an identified gap will set off bells with auditors and regulators.
- Repair, add and enhance where possible within the parameters of your risk assessment. Prepare thorough documentation as to the rationale for why identified gaps were not filled, or the plans and timeline for closing those gaps. Always be working on developing or finding a solution to a problem. Prepare interim mitigations if possible until a long-term solution can be successfully implemented.
- Stay abreast of industry best practices and integrate them into your program where applicable. Auditors will look for this.
- Acknowledge the fact that it is an auditor's job to find issues. Accept the likelihood that they will find something to cite even in the best of compliance programs. No compliance program can be perfect. Even the regulators do not expect perfection. Lack of perfection means there will always be policies or procedures to enhance, add or streamline.

Preparing for an audit is a constant process that should be continually assessed and honed

Audit management


- Come to an agreement with the auditors on the scope of the audit before the audit starts and document it with appropriate signatures. This can help prevent scope creep and misunderstandings with the auditors. If the scope is changed during the audit, ensure the auditors make the change in writing and that it is kept on file.
- If necessary, provide education for the auditors, especially if your program has unique aspects and requirements. It is particularly important to be able to document thoroughly why a particular regulation or best practice does not apply. Simply saying it does not apply, even if it is obvious to you, rarely meets an auditor's requirements.
- Every industry and many organizations have their own jargon that may not match the industry standard terminology. The best remedy is to adopt industry-standard language. If not, prepare a glossary of terms unique to your organization and their common counterparts. Have this ready at the start of the audits to avoid misunderstandings during the audit process.
- It is always better to acknowledge an issue than to marginalize it or attempt to hide it. Auditors do not take kindly to someone trying to hide a deficiency.
- Work closely with the auditor to clarify any unanticipated data or documentation requests. Ensure you agree on the content and parameters of the test before providing the data. An auditor could possibly misidentify provided information that does not meet their expectations as an attempt to stall or cover up program issues. At worst, it will extend the audit process until their needs are met. If responding to an audit request is not possible, be prepared to provide a detailed explanation as to why. Explore if alternates that are readily available would meet their needs. If your audit scope process was good, unanswerable requests should be identified and dealt with early in the process. Also, if your audit preparation was solid, you likely already have most potential requests covered and ready to be provided.
- Provide facts not opinions, as covered in the audit preparation. Opinions as to whether a policy or procedure is effective or whether a government regulation is logical is immaterial in an audit and will likely cause problems. Interactions with auditors should be professional, dispassionate and measured. The audit is about the program, not personal feelings.
- If the auditor identifies a deficiency during the audit, it would be advisable to create a preliminary action plan and present it before the audit is completed.

Post-audit actions

- Learn from every audit experience, whether it was routine or painful. Identify and improve audit elements that were less than satisfactory. If you do not, it is likely that you will suffer the same negative experience in subsequent audits. In the worst case scenario, your organization is hit with fines and penalties. Review your team's performance objectively. Allowing frustrations and negative feelings about the process to affect any audit response or even the next audits will be counterproductive.

- If you did your homework before the audit there should be few, if any, findings that come as a surprise. That means your response should not have to be created from scratch. Ensure that you correct any misunderstandings or perceptions in the findings. This does not mean that the auditors will accept your response. However, not responding to issues might be seen as an acknowledgement of a deficiency, which could create an ongoing issue in future audits.
- Plan and implement any necessary corrective actions well in advance of the next audit. Scrambling to respond to earlier audits just before the next one will not only degrade the audit preparation but will likely result in deficient mitigations. No auditor will look kindly upon previous recommendations that are not given full attention, either through implementation or developing a thorough explanation as to why the recommendation was not implemented.
- Ensure that the results of your regulatory audits and your corrective actions are made available to future internal or third-party auditors. Their findings will likely help you determine if your response to the official audit was satisfactory.
- Stay ahead of audits in the planning process. Audits are an integral part of any compliance program, so make it part of your annual planning, budget and organizational culture of compliance. Developing a set of preparatory procedures would likely prove useful but should be separate from your compliance procedures and proprietary.
- When it comes to audits, prepare, manage, respond and repeat.

Conclusion

Successfully surviving an audit requires a management process partnered with a dedicated team effort. It is a professional report card from a demanding teacher. The results can range from a job well done (until next time) to a frank assessment of your organization's commitment to compliance. In fact, surviving is the lowest acceptable outcome. One should be able to approach an audit confidently and with an open mind. The recommended actions in this article are hardly great revelations. Like many other requirements in the business world, they are grounded in common sense and the dedication to knowing one's responsibilities and performing them to the best of one's ability. Solid preparation, wise management and dedicated follow-up will enable you to save your energy for real challenges like the budget process. 

Ed Beemer, CAMS-FCI, efb@compliancecomm.com

Lauren Hughes, CAMS-FCI, laurenhughes81@gmail.com

Best crisis management practices for data breaches: Part one



In recent years, many companies have had to respond to a crisis related to unauthorized access to confidential information. These data breaches are not the only crises an organization may face. COVID-19 forced organizations to activate their crisis management plan or develop one in the heat of the moment. What would happen if the media reported, despite all the precautions in place, that a major client with a direct link to a terrorist group or a previously unknown organization was trying to launder money? Naturally, know your customer and risk management processes would have to be reviewed. But what should be done when the news gets out?

Data breaches cause significant costs. The Ponemon Institute reveals that a data breach costs an average total of \$3.86 million that breaks down as follows: \$1.11 million for detection and escalation costs, \$1.52 million for lost business costs, \$240,000 for notification costs and \$990,000 for ex-post response costs.¹ The costs related to lost revenue are the most significant, representing approximately 40% of the total. The same report points out that the average costs decrease by almost \$2 million if the company has an incident response team and if they conduct incident response testing.

The objective of this two-part article is to review best practices for crisis management and to identify some interesting data. Even if the best practices can be applied to any type of crisis, this article will focus on crises during unauthorized data breaches.

Experts unanimously agree on some points while on others, the debate persists. The first finding from experts is that it is necessary to be prepared. As the saying goes, it is not if, but when such a breach will occur.

In the context of a data breach, information security, computer security, control measures, privacy policies and training sessions are must-do activities. In fact, it is important to create a “culture of security.”² Far from wanting to sideline these dimensions, this article will instead emphasize other aspects of the crisis management process.

Preventive activities (pre-crisis)

The preparatory activities for a crisis are multiple; they affect different departments and, of course, involve senior management. Sometimes these activities are technical (appropriate management control measures or activities specific to IT security), sometimes financial (purchase of cyber insurance³) and sometimes more strategic (overall risk management and compliance).

The following are the best practices in the context of crisis prevention:

- Creating a crisis management team
- Establishing a crisis management plan
- Developing a communications plan

Creation of a crisis management team

One of the first preventive activities in crisis management is to set up a multidisciplinary crisis management team and identify backups in case of travel or vacation.⁴ This will involve clarifying the roles and responsibilities of each member of this team and identifying the person in charge.⁵ The following would be the main tasks of this team:⁶


- Establishing the crisis management plan (or updating it)
- Training each team member and all employees on the crisis management plan
- Simulating different crisis scenarios

Given the strategic importance of crisis management, a member of senior management should be part of the team.⁷ In addition to concretizing senior management support, this person will be the point of contact with executives and board members. Experian emphasizes that the “involvement of the executive team greatly determines the success of a data breach response plan...creating a culture of cybersecurity.”⁸

There are mixed views on the composition of a crisis management team. However, in the context of a data breach, the team should at least include:

- A member of senior management
- An IT (or security) specialist
- A legal advisor
- A public relations specialist
- A person responsible for human resources

In addition, this team should have a discretionary budget to consult or hire external resources as needed. When a crisis occurs, this is not the time to negotiate these resources and chase approvals.



One of the first preventive activities in crisis management is to set up a multidisciplinary crisis management team and identify backups in case of travel or vacation

Establishment of a crisis management plan

Once the roles and responsibilities are assigned, the next step is to establish the crisis management plan (CMP). As Experian states, “response plans are a critical component of any business’s cyber security strategy.”⁹ Not only will this plan guide the actions of the organization’s members, it will also reduce the response time and the financial impacts.¹⁰ Because threats, the economic environment and technologies are constantly changing, the CMP should be updated regularly.¹¹

The following are the main sections of a CMP:¹²

- The names and functions of the crisis management team members as well as information regarding replacements and the identification of the person in authority
- The roles and responsibilities of the crisis management team members
- The procedures to be followed
- The points of contact for external stakeholders (e.g., credit bureaus, law enforcement officers, regulatory authorities, external legal counsel, investigative firms specializing in breach situations, business partners who could potentially be affected)
- The communications plan (see below)
- A contingency plan for business continuity

Given the rise in ransomware, planning an organization’s response to such threats and training employees who may face these situations are suggested.¹³ In addition, opening a cryptocurrency account, considering it is a preferred method of payment in these types of crimes, is also recommended.¹⁴

All these steps will save time and restore normal functionality of the organization as quickly as possible. Finally, having members of the crisis management team keep hard copies of the CMP in strategic locations would be an excellent idea, as denial-of-service attacks can block access to the system for an extended period of time.

Development of a communications plan

One of the most important preventive activities is to plan what the organization’s spokesperson will say publicly following a breach.¹⁵ The words, the tone of the message and the speed of response are strategies that will protect the organization’s reputation and potentially reduce the financial impact.

The communications plan should at least include:

- The names and duties of the communications’ team members, their alternates and the person in authority
- An official spokesperson for the organization who is a public relations specialist
- The roles and responsibilities of the members of the communications team



One of the most important preventive activities is to plan what the organization’s spokesperson will say publicly following a breach


Other elements of the communications plan include:¹⁶

- Preparing a pre-approved crisis website that will be activated, completed and updated at the time of a crisis in advance
- Preparing pre-approved drafts of senior management news releases that will be adapted upon the occurrence of the crisis
- Preparing pre-approved public (regulatory) announcements that will meet regulatory compliance requirements
- Conducting fictitious briefings to be well-prepared in such circumstances. As stated by Bill Rosenthal, CEO of Communispond, “Be ready to answer tough questions.”¹⁷

The communications plan will need to address how to notify employees, individuals whose personal information may have been compromised, the media, appropriate authorities and business partners including the major credit bureaus (Equifax, Experian and TransUnion):

- For employees, the intranet remains the best means of contact. They should be informed as soon as possible, especially those working in call centers.¹⁸ According to Coombs, “well informed employees provide an additional channel of communication for reaching other stakeholders.”¹⁹ The intranet could also be used to contact business partners.
- As for victims (alleged and potential), several avenues exist: the newly activated website, their current accounts, emails, personalized letters, traditional media and social media. It is recommended to “take [all] steps to preserve customer trust and loyalty.”²⁰

To summarize, data breaches are costly and will not disappear. The first part of this article pointed out the need for organizations to be prepared. Such preparedness is achieved by creating a crisis management team with well-defined responsibilities and by establishing a sound and updated crisis management plan (procedures and external points of contact), which includes both communications and contingency plans.

The second part will cover best practices in response to a crisis, discuss follow-up activities and present some takeaways. 

Claude Mathieu, Ph.D., professor, head of the graduate program in the fight against financial crime, Université de Sherbrooke; co-chair, ACAMS Montreal Chapter, Canada, Claude.Mathieu@USherbrooke.ca

William Poisson, M. Adm, CISSP, CISA, CISM, CFE, graduate student, master of administration program, concentration in fight against financial crime, Université de Sherbrooke, Canada

Yves Trudel, Ph.D., professor, director of MBA and master programs, Université de Sherbrooke, Canada, Yves.Trudel@USherbrooke.ca

¹ “Cost of a Data Breach Report 2020,” IBM, July 2020, <https://www.ibm.com/security/data-breach>

² Ramakrishna Ayyagari, “An Exploratory Analysis of Data Breaches from 2005–2011: Trends and Insights,” *Journal of Information Privacy and Security*, <https://www.tandfonline.com/doi/abs/10.1080/15536548.2012.10845654>; “Protecting Personal Information: A Guide for Business,” *Federal Trade Commission*, October 2016, <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>

³ “Cybersecurity Insurance,” *Cybersecurity & Infrastructure Security Agency*, www.dhs.gov/cisa/cybersecurity-insurance (accessed May 5, 2021); “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” *Experian and Ponemon Institute*, February 2018, https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon

⁴ *Ibid.*; Theodore J. Kobus III, “2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World,” *BakerHostetler*, April 3, 2019, <https://www.bakerdatacounsel.com/data-security-incident-response/fifth-annual-data-security-incident-response-report-released-managing-enterprise-risks-in-a-digital-world/>

⁵ “PwC’s Global Crisis Survey 2019,” PwC, 2019, <https://www.pwc.com/ee/et/publications/pub/pwc-global-crisis-survey-2019.pdf>; Jena Valdetero and David Zetoon, “Data Security Breach Handbook for Hotels, Venues, & the Hospitality Industry,” *Bryan Cave*, 2016, <https://www.lexology.com/library/detail.aspx?g=d26e57fb-a72e-4d35-a147-1a5bb913b7f0>

⁶ Theodore J. Kobus III, “2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World,” *BakerHostetler*, April 3, 2019, <https://www.bakerdatacounsel.com/data-security-incident-response/fifth-annual-data-security-incident-response-report-released-managing-enterprise-risks-in-a-digital-world/>; “Best Practices for Victim Response and Reporting of Cyber Incidents,” *U.S. Department of Justice*, September 2018, <https://www.justice.gov/criminal-ccips/file/1096971/download>; “Data Breach Response Guide,” *Experian*, 2018–2019, <https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf>; Katelyn Smith, “Best Practices for Effective Corporate Crisis Management: A Breakdown of Crisis Stages through the Utilization of Case Studies,” *California Polytechnic State University*, March 2012, <https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1045&context=joursp#:text=The%20first%20best%20practice%20for,98>

⁷ “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” *Experian and Ponemon Institute*, February 2018, https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon

⁸ “Data Breach Response Guide,” *Experian*, 2018–2019, <https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf>, 6.

⁹ *Ibid.*, 4.

¹⁰ “Best Practices for Victim Response and Reporting of Cyber Incidents,” *U.S. Department of Justice*, September 2018, <https://www.justice.gov/criminal-ccips/file/1096971/download>

¹¹ *Ibid.*; “Data Breach Response Guide,” *Experian*, 2018–2019, <https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf>; “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” *Experian and Ponemon Institute*, February 2018, https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon

¹² “Crisis Management and Communications,” *Institute for Public Relations*, October 30, 2007, <https://instituteforpr.org/crisis-management-and-communications>. “Barton (2001), Coombs (2007a), and Fearn-Banks (2001) have noted how a CMP saves time during a crisis by pre-assigning some tasks, pre-collecting some information, and serving as a reference source.”

¹³ Theodore J. Kobus III, “2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World,” *BakerHostetler*, April 3, 2019, <https://www.bakerdatacounsel.com/data-security-incident-response/fifth-annual-data-security-incident-response-report-released-managing-enterprise-risks-in-a-digital-world/>; “Best Practices for Victim Response and Reporting of Cyber Incidents,” *U.S. Department of Justice*, September 2018, <https://www.justice.gov/criminal-ccips/file/1096971/download>

¹⁴ “BakerHostetler 2017 Data Security Incident Response Report Based on 450 Incidents,” *BakerHostetler*, 2017, <https://www.databreaches.net/bakerhostetler-2017-data-security-incident-response-report-based-on-450-incident/>

¹⁵ Bokyoung Kim, Kristine Johnson and Sun-Young Park, “Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity,” *Cogent Business & Management*, July 24, 2017, <https://www.tandfonline.com/doi/full/10.1080/23311975.2017.1354525>; Katelyn Smith, “Best Practices for Effective Corporate Crisis Management: A Breakdown of Crisis Stages through the Utilization of Case Studies,” *California Polytechnic State University*, March 2012, <https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1045&context=joursp#:text=The%20first%20best%20practice%20for,98>

¹⁶ “Data Breach Response Guide,” *Experian*, 2018–2019, <https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf>; “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” *Experian and Ponemon Institute*, February 2018, https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon

¹⁷ Nate Lord, “Data Breach Experts Share the Most Important Next Step You Should Take After a Data Breach in 2019 & Beyond,” *Data Insider*, August 11, 2020, <https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015>

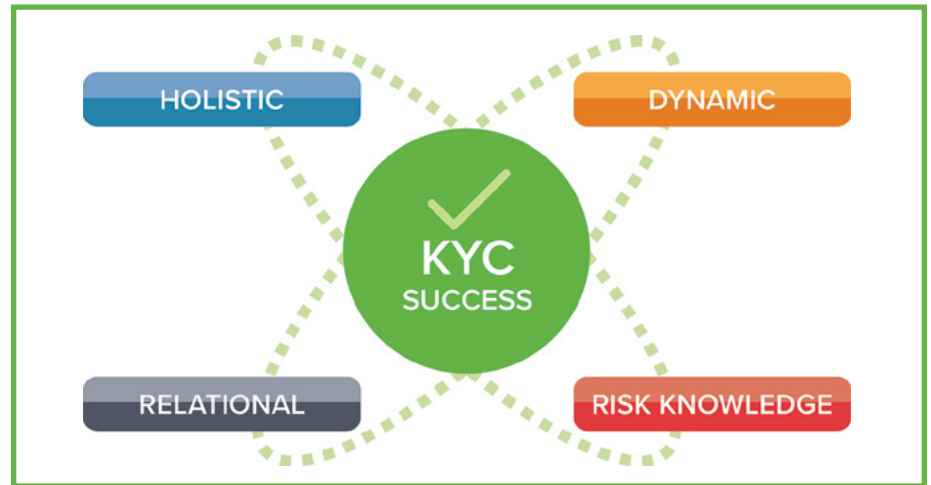
¹⁸ Katelyn Smith, “Best Practices for Effective Corporate Crisis Management: A Breakdown of Crisis Stages through the Utilization of Case Studies,” *California Polytechnic State University*, March 2012, <https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1045&context=joursp#:text=The%20first%20best%20practice%20for,98>

¹⁹ “Crisis Management and Communications,” *Institute for Public Relations*, October 30, 2007, <https://instituteforpr.org/crisis-management-and-communications/>

²⁰ “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” *Experian and Ponemon Institute*, February 2018, https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon,2

The right data for **KYC** **SUCCESS**



Figure 1: Elements of KYC success

In today's world of financial crime compliance, there is a concerted effort from regulators to push the limits—at least in the minds of many know your customer (KYC) and anti-money laundering (AML) practitioners—on KYC requirements. More and more, there have been expectations to use the abundance of data available regarding customers. However, simply adding data requirements does not guarantee the achievement of the end goal: a robust AML compliance regime and for financial institutions, one that meets regulatory requirements and does not stand in the way of business growth.

To achieve the end goal, there must be a paradigm shift in the way KYC is conducted. Specifically, AML professionals must consider not only the collection and collation of individual data elements, but also the missing data elements that can be identified only when looking at the human decision-making processes around each data element and the relationships among the data elements.

Before discussing what constitutes the right data for KYC success, KYC success must be defined—in both today's terms and tomorrow's.

What is today's definition of "KYC success"?

To date, "KYC success" seems to be measured by the quantity of data collected. In some instances, there may be a focus on the collation and presentation of that data. It has also been defined by the speed and efficiency with which the data is collected and collated. It is as if the old-fashioned "weight test" is being applied to KYC—the more data one has, the better the compliance. And therein lies the issue; there has been a focus on compliance—and the cost of compliance—and not on making the right decisions on the right customers in a way that will enhance revenue for businesses.

What is tomorrow's definition of "KYC success"?

Tomorrow's definition of KYC success needs to focus on four key program elements: it must be holistic, dynamic, relational and include a clear understanding of risk and how all of these elements interact (see Figure 1). KYC success will lead to a better understanding of prospective and current customers. That must include bringing together, holistically, the data collected and doing so in a dynamic, real-time way. It means understanding the relationships across applications and processes that exist between data elements in currently disparate systems and processes. It means understanding the risks presented by the customer and how those risks change over the life cycle of the customer.

Now some will say that it is already being done but the focus has mainly been on the collection of complete, accurate and timely data used in decision making, not on making the decision. Specifically, there has not been a focus on the data elements that describe the relationships between the data currently being collected and how those data elements and data relationships drive a determination of customer risk.

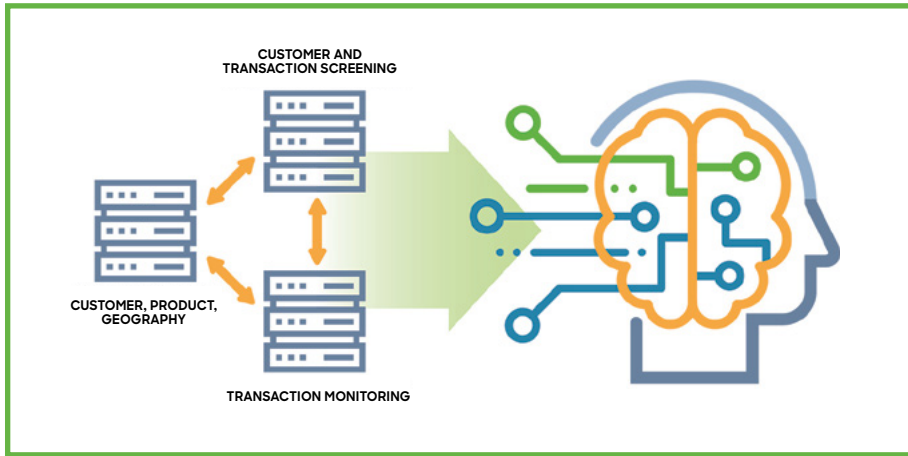
The answer to tomorrow's KYC success is not more data but rather data that can be understood and informative. It is data that is holistic, dynamic and relational, brought together in a way that can identify those customers whom you want to onboard and/or with whom you want to expand your relationship.

How to move from today to tomorrow

In today's world of AML silos, start by examining, determining and understanding, in the context of human decision making, how all the data elements in the three main AML areas—sanctions screening, transaction monitoring and KYC—fit together to portray the customer (see Figure 2).

Begin by looking at the data elements collected individually within the defined silos. Then look at data characteristics or elements that define the relationship between and among data elements, not only within the silos but then, critically, between and among those silos, to create a holistic view. Clearly, there is a need for good, if not high, quality data as part of this exercise, but the relational aspects must be defined in the context of human decision making.

Figure 2: The three main areas of AML



A basic example of this would be in the context of anticipated normal activity and the relationship of that activity to customers that are similarly situated—and to the transactions of both the customer in question and similarly situated customers. Today, data is collected typically by interviewing the customer or prospective customer and asking them what they expect to do. This is dutifully logged in a KYC file and a box is checked stating that this information was acquired. It is left to the KYC analyst—who may or may not be a subject-matter expert and likely is not one for the customer, industry and transaction types—to decide whether the anticipated normal activity is indeed normal.

In this scenario, there is no mechanism to collect and assess other data elements to corroborate or otherwise support the information provided by the customer. Reliance is placed on the KYC analyst or the case investigator to seek out and assess the activity in this context.

Yet there is a plethora of data that is likely already available within the KYC file. For example, for larger customers, annual, quarterly or other reports have likely been obtained to “substantiate” the company. What data can be gleaned from such reports that would either substantiate or perhaps predict anticipated normal activity? The challenge is in reading, identifying, extracting and analyzing

these additional data elements to form a deeper, more comprehensive picture of the customer’s activity.

The shift to tomorrow is a paradigm shift in the thinking around KYC data

Not only does KYC need to change from a data collection and operational perspective, but new questions must be asked regarding KYC data. Those new questions need to be focused beyond regulatory requirements to the value of KYC data. That value can be a predictive focus, such as a credit or a marketing perspective.

For example, if looking at KYC from a perspective such as lending (i.e., credit), begin looking across the customer to assess them as solid and trustworthy, someone with whom business can be




conducted. Look at the customer from the perspective of what they have done as an indicator of what they may do. Also, look at KYC from a marketing perspective, i.e., ask questions about what the customer likes or what they will likely do since what they are doing now may also be an indicator of future actions. This perspective should become integrated into the KYC anti-financial crime thinking because what the customer may do may be outside the norm and worthy of investigation and potential reporting.

The new AML officer

To achieve this paradigm shift there must be new thinking on the part of the AML officer. That new thinking encompasses all data that is available today, but more importantly, all data regarding the relationships among current data elements. It must also encompass an understanding of the decision-making processes in place today and going forward as well as what and how data describe that decision-making process. Only then can the right data be presented to a KYC analyst to use in the decision-making process—or perhaps more importantly, to be used by artificial intelligence to present a likely decision for confirmation by the KYC analyst.

The “new” AML officer must also think beyond simply meeting the regulatory requirements of the day. Obtaining and using the right KYC data does cost money. The new AML officer must think in the context of the business and how the right KYC data is a business enhancement and not just another requirement.

With the right thinking on the part of the new AML officer, AML professionals can finally achieve that utopian world depicted in the statement “I’m from compliance, and I’m here to help!” 

Steve Marshall, director, FinScan Advisory Services, Innovative Systems, Inc./FinScan, PA, USA, smarshall@innovativesystems.com

How granular can you get with your matching rules?

See the power of a
Risk-based Approach in Sanctions & PEP Screening

MATCHING RULE SCENARIOS

“One Size Fits All”



- Same matching rules for all Sanctions and PEPs

Risk-based Approach

M O R E G R A N U L A R



- **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

Twenty impacts over 20 years

A CAMS Today is kicking off the celebration of ACAMS' 20-year anniversary with a list of the 20 most transformative anti-financial crime (AFC) events of the last 20 years. The editorial team asked ACAMS advisory board co-chair Rick Small, CAMS, and former ACAMS advisory board member Lauren Kohr, CAMS-FCI, for their input.



Small leads the financial crimes team for Truist, which includes managing anti-money laundering (AML) compliance, controls and investigations, fraud management and the financial investigations resulting from cyber events. He joined BB&T, now Truist, in 2016 as the first financial crimes program director.

Small has over 35 years of experience in the public and private sectors. Before joining BB&T, he was the senior advisor for AML and financial crimes with EY; senior vice president, enterprise-wide AML, anti-corruption and international regulatory compliance for American Express; and the AML leader for GE Money, a division of General Electric. Small began his private sector career as managing director, global AML for Citigroup.

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



Kohr's background includes more than 16 years of experience in the AFC sector with significant experience in Bank Secrecy Act/anti-money laundering (BSA/AML) and sanctions compliance, managing complex regulatory issues and remediation projects, and facilitating public and private partnerships to develop effective strategies to combat illicit financial activities. Currently, she serves as the senior director, AML of Americas for ACAMS. As the senior director, Kohr is focused on building the global Anti-Financial Crime Task Force focused on public-private partnership engagement, assisting in executing the global law enforcement strategy, and serving as both a subject-matter and technical expert on anti-money laundering/counter-terrorist financing (AML/CTF), regulatory policy and AML regime priorities. Previously, she served as the senior vice president, chief risk officer and BSA officer at Old Dominion National Bank (ODNB) in Tysons Corner, Virginia. In this role, Kohr was responsible for ODNB's enterprise risk management program, including leading the bank's BSA/AML and Office of Foreign Assets Control (OFAC) program.

Before her role at ODNB, Kohr served as the vice president/director of AML/BSA/OFAC at Metro Bank in Harrisburg, Pennsylvania. During this time, she was responsible for developing, implementing and overseeing all aspects of the Bank Secrecy Act (BSA) compliance program, including the USA PATRIOT Act, AML and OFAC regulations. Kohr was the 2016 ACAMS AML Professional of the Year, won the 2016 ACAMS Today Article of the Year Award and was awarded the U.S. Capital Excellence in Public/Private Partnerships in 2019. She is a frequent speaker at numerous conferences, both domestically and internationally, for the public and private sectors on AML, BSA, OFAC and counter-terrorist financing (CTF)-related topics. Kohr serves on the ACAMS U.S. Capital Chapter board of directors, AML Partnership Forum board of directors and is part of the Empowering Together: Women in AML initiative. She also previously served on the ACAMS advisory board.

As subject-matter experts in their respective fields and as well-known orators in the AFC space, Small and Kohr shared with ACAMS Today what they thought were the top 20 most significant AFC developments over the past two decades. During the discussion Small and Kohr mentioned similar items on their list. ACAMS Today took their valuable input and combined their lists to bring you the top 20 most transformative items in the past 20 years:

1. September 11, 2001
2. USA PATRIOT Act
3. The Federal Financial Institutions Examination Council BSA/AML Examination Manual
4. Enhanced private-public partnerships
5. Financial institution industry engagement with combating human trafficking and assisting human trafficking survivors
6. Broad expansion of AML to include CTF
7. Broad expansion of AML to include cybercrime
8. Broad expansion of AML to include fraud
9. Financial institution industry engagement with not-for-profits to provide guidance and banking services for nongovernmental organizations and nonprofit organizations
10. Customer due diligence regulation
11. Beneficial ownership requirements
12. Anti-Money Laundering Act of 2020
13. Release of the first-ever AML national priorities
14. The rise of fintechs as an alternative to traditional banks to provide banking-related services
15. Digital currencies to include cryptocurrency, virtual currency and informal value transfer systems
16. AML technology to include big data, artificial intelligence, machine learning and automated transaction monitoring systems
17. Identification of money flow tied to social impact issues, such as environmental crime
18. Trade-based money laundering
19. The complexity of sanctions evasion schemes
20. COVID-19 pandemic


Finally, both Small and Kohr shared their thoughts on what the next 20 years could hold for the AFC industry. Small stated the following, “In the next 20 years, I would expect that emerging technology is going to significantly blossom and provide cutting edge technology solutions to manage AML risks.”

Kohr added, “In the next 20 years the focus will be to:

- Continue to find more effective and innovative ways to combat money laundering, terrorist financing and proliferation financing
- Evolve public-private partnerships and opportunities to share information
- Position the AFC community to be both proactive and reactive in combating these heinous crimes
- Go above and beyond, do more than our part, expand our thinking beyond the norm

We all must play our part and find ways to evolve the AFC community and its initiatives; and not find reasons why we can't or let barriers and challenges prevent us from trying. We can do it.”

As we begin the 20-year celebration of ACAMS, we also want to remember and honor the 2,977 people who lost their lives on 9/11 during the most horrific terrorist attacks on American soil. In addition, we would like to remember and thank the dedicated first responders who ran toward danger to save their fellowmen on that fateful day.

ACAMS Today is grateful to be a part of a community and industry that is fighting to end financial crime and everything it encompasses. We hope you will join us as we continue celebrating 20 years of ACAMS from now and into 2022. 

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

Stephanie Trejos, CAMS, editor, ACAMS, FL, USA, strejos@acams.org

Ransomware: The digital battleground



In the age of the internet, a hack meant the loss of personally identifiable information (PII). In the 2018 hack of Facebook, 50 million users found their birthdates, education, location and other PII vulnerable to cybercriminals.¹ According to chief executive officer Mark Zuckerberg—whose own account was compromised—attackers would have had the ability to view private messages or post on someone’s account but they did not have access to financial data.

Fast forward to the age of crypto, the internet of money, where a hack not only means the potential loss of PII but it could also mean the loss of life savings—think theft at the speed of the internet. It has also meant the proliferation of ransomware-as-a-service (RaaS) providers, online terrorist fundraising, programmatic money laundering and cyberattacks by nation state actors at an unprecedented speed and scale. The May 2021 ransomware attack on the Colonial Pipeline not only caused lines at gas stations up and down the east coast of the U.S., it also caused a shift in national security policy and a recognition by law enforcement and policymakers that the battle has shifted online.

Colonial Pipeline: A case study

On May 7, Colonial Pipeline, the company that operates a 5,500-mile pipeline that delivers 45% of the gasoline and jet fuel to the U.S. east coast, fell victim to a ransomware attack. In response to the attack, Colonial proactively shut down its operations causing fuel shortages and long lines at gas stations from Miami to New York. Some schools even went virtual in response to the attack.

On May 10, *The New York Times* reported that the FBI confirmed that the DarkSide ransomware was responsible for compromising the Colonial Pipeline networks.²

DarkSide is a RaaS provider that sells its malware on the darknet and gets a cut from the buyer’s profits for the use of the malware. What is ransomware and RaaS? Ransomware is a type of malicious software that cybercriminals use to block a victim from accessing their own data. These cybercriminals access a victim’s systems and encrypt files holding the data hostage until the demanded ransom is paid. After the initial infection, the ransomware may attempt to spread throughout a victim’s network to shared drives, servers, attached computers and other accessible systems. RaaS allows illicit actors (without coding experience) to launch ransomware attacks. Think of it as a cybercriminal McDonald’s where “franchisees” can purchase RaaS kits—readily available on the darknet with the Tor Browser. The RaaS developer takes a franchise fee that includes a percentage of profits (typically 20%-30%). In return, the RaaS

developer provides a brand, training, equipment and 24/7 support. No expertise necessary. Often these ransom payments are demanded and paid in cryptocurrencies such as Bitcoin.

But ransomware was around long before cryptocurrencies. As early as 2005, illicit actors set up shell companies to receive credit cards, prepaid cash cards and gift cards for payments. While cryptocurrencies are not responsible for ransomware, the low cost, speed and pseudonymity of crypto payments make crypto the go-to currency for cybercriminals.

Following the attack on the Colonial Pipeline, Anne Neuberger, deputy national security adviser for cyber and emerging technology, held a White House briefing on May 10. She described the attack as “ransomware as a service variant” in which “criminal affiliates conduct attacks and then share proceeds with the ransomware’s developers,” and confirmed that the FBI had been investigating DarkSide since October.³ In addition to locking the Colonial Pipeline’s computer systems, including the company’s billing system which left it unable to track fuel distribution and billing, DarkSide also stole over 100 gigabytes of corporate data.⁴

On Thursday, May 13, nearly a week after the attack, reports emerged that Colonial paid a 75 bitcoin (BTC) ransom—worth as much as \$5 million, allowing the company to restore service on Wednesday, May 12.⁵ On May 8, 75 BTC were withdrawn from a U.S.-based exchange and shortly after transferred to DarkSide’s ransomware payment address.⁶ The funds were soon cleared into DarkSide’s Bitcoin wallet.

On Friday, May 14, things went dark for DarkSide. According to Intel 471, DarkSide told affiliates it had lost access to its own infrastructure and would be closing, citing disruption from law enforcement and pressure from the U.S. DarkSide added that funds from their payment server were transferred to an unknown account as part of a “seizure.”⁷ On May 13, 113.5 BTC were withdrawn from DarkSide’s wallet and placed into a different wallet.

On June 7, a month after the attack on Colonial, the U.S. Justice Department (DOJ) announced that it had successfully seized 63.7 bitcoin (\$2.3 million) from the cryptocurrency wallet that held the ransomed funds. A seizure warrant was filed in the Northern District of California.⁸ “Earlier today, the Department of Justice has found and recaptured the majority of the ransom Colonial paid to the DarkSide network in the wake of last month’s ransomware attack. Ransomware attacks are always unacceptable, but when they target critical infrastructure, we will spare no effort in our response,” Deputy Attorney General Lisa Monaco said at a news conference.⁹

In a press release, Monaco stated, “Following the money remains one of the most basic, yet powerful tools we have. Ransom payments are the fuel that propels the digital extortion engine, and today’s announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises.”¹⁰

But following the money only takes law enforcement so far. Blockchain analytics are powerful tools that allow law enforcement to track and trace the flow of funds on the open blockchain in ways that have revolutionized financial crime investigations. However, while blockchain analytics are able to track the movement of cryptocurrencies, these tools are not able to seize illicit funds. When DOJ announced in its press release that “by reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin...to a specific address, for which the FBI has the ‘private key,’”¹¹ the questions on everyone’s lips was, “How did FBI crack the private key and seize the illicit proceeds?”

There are likely a number of possible scenarios—from the use of technology to reliance on human intelligence. As *The New York Times* reported, “The FBI did not appear to rely on any underlying vulnerability in blockchain technology, cryptocurrency experts said. The likelier culprit was good old-fashioned police work.” *The Times* continued, “Federal agents could have seized DarkSide’s private keys by planting a human spy inside DarkSide’s network, hacking the computers where their private keys and passwords were stored, or compelling the service that holds their private wallet to turn them over via search warrant or other means.”¹² The bottom line is that the seizure comes down to great police work. Whether high tech or human, the seizure was likely the result of months of great investigative work. As the White House mentioned in its first press conference on DarkSide, the FBI had been looking into DarkSide since October. While the bitcoin

seizure happened quickly, it was likely the result of months or years of work across the interagency, and around the globe, to build networks of ransomware providers and cybercriminals.

What does Colonial Pipeline mean for the future of U.S. national security policy?

In the wake of the Colonial Pipeline cyberattack, FBI Director Christopher Wray compared recent cyberattacks—such as those on Colonial and JBS Foods, the world’s largest meat supplier—to 9/11, telling *The Wall Street Journal*, “There are a lot of parallels, there’s a lot of importance, and a lot of focus by us on disruption and prevention.”¹³ On the previous day, the DOJ elevated cyber intrusions to the level of counter-terrorism investigations, instructing U.S. attorney’s offices across the country to coordinate cases involving ransomware, cyberattacks, counter anti-virus services, illicit online forums or marketplaces, cryptocurrency exchanges, bulletproof hosting services, botnets and online money laundering services with the newly created Ransomware and Digital Extortion Task Force.¹⁴ This shift by law enforcement could signify the first shift in national security policy in over 20 years—a recognition that this is now a post post-9/11 moment where terrorists, cybercriminals and rogue nation state actors have taken to the digital battlefield.

What compliance teams and the private sector can do to prevent cyberattacks

Arguably the best lessons come from the great movies of the 1980s and cyber defense is no exception. President Ronald Reagan, after having just screened compliance must-watch *WarGames*—the 80s classic starring Matthew Broderick who unwittingly hacks into a military supercomputer and almost starts WWII—famously charged the National Security Agency with hardening the nation’s cyber defense for government, business and personal systems.¹⁵ And that work is still ongoing.

Any discussion about the approach to taking on illicit actors who engage in ransomware and other cyberattacks involves a discussion of public-private partnerships at a global scale.¹⁶ Critical infrastructure like Colonial Pipeline and JBS Foods are controlled by private sector entities. On June 2, 2021, deputy national security advisor Anne Neuberger penned an open letter to the private sector outlining ways in which private sector companies can harden their defenses against ransomware attacks.¹⁷ Specifically, the letter urges the private sector to immediately take the actions described in Figure 1.

The approach to ransomware, proactive and reactive, is a whole of business approach. It starts with educating employees not to click on links or unknown webpages in spam emails. The most common source of a ransomware attack is a phishing email.¹⁸ The email typically relies on social engineering—an attack using human psychology, rather than technical hacking methods—to gain access to computer systems. The attacker relies on social interaction, not high-tech hacks, to manipulate employees into handing over systems access. Once the employee clicks on the link, the malware takes over, spreading to connected systems and searching for valuable data.

While much of the focus for the private industry involves a proactive approach to cyber hygiene and hardening computer systems and protocols, being ready to react in case of an attack is also critical. In a recent interview, Lisa Sotto, head of the cybersecurity practice at Hunton Andrews Kurth, explained the following,

“One important way a company can mitigate harm in the event of a security breach is to take proactive steps in advance of an incident. It is critical to have an up-to-date incident response plan that has been practiced through tabletop exercises. Companies should have well-rehearsed incident response teams composed of members who know their various roles and responsibilities should a breach occur.”

Figure 1: The U.S. government's recommended best practices to protect against the threat of ransomware

Implementing the best practices outlined in President Biden's Executive Order on Improving the Nation's Cybersecurity: These practices include: (a) the use of multi-factor authentication instead of relying on passwords alone; (b) the use of network detection and response technologies to actively detect and hunt for malicious activity on a network and stop it before it can damage the network or systems; (c) the use of encryption technology to minimize the damage if the ransomware not only holds data hostage through encryption but also exfiltrates the information to attempt to further extract a ransom by threatening to disclose sensitive information even when the data was restored from backups; and (d) use an appropriately qualified system security team that monitors available information for new threats and that appropriately patches and maintains the business's IT systems to protect against these threats.

Backup system images, configurations, and data to offline storage and regularly test these backups: Ransomware will regularly try to encrypt and delete backups accessible from the business network. Accordingly, backups should be stored offline where they cannot be reached in a ransomware attack that encrypts the business's IT systems. Furthermore, businesses are advised to regularly test whether the backups are sufficient to restore the system in the event of an attack.

Promptly patch and update systems: As new vulnerabilities are discovered, patching is a critical component in protecting against ransomware attacks. Organizations should consider a patch management system and use a risk-based assessment strategy to determine when to patch operating systems, applications and firmware.

Test incident response plans: Businesses should have an incident response plan and test it regularly through tabletop simulations to uncover and address any gaps in the plan. When reviewing

the incident response plan, the business should ask itself several core questions, including (a) what systems are critical to continuing business operations; (b) how long can the business continue operations without specific systems; and (c) would the business be forced to discontinue manufacturing operations if specific business systems were affected by a ransomware attack (such as billing). The business should then adjust the incident response plan as appropriate.

Check the security team's work: Companies should test their systems' security through penetration testing and other vulnerability testing.

Network segmentation: Ransomware attacks can steal data and disrupt operations. For businesses that engage in manufacturing and production operations, ransomware attacks can significantly impact if ransomware can get to the systems that control manufacturing and production. The letter recommends that the computer networks that control manufacturing and production operations be separated from the networks used for corporate business functions and that businesses identify the links between these networks and carefully filter and limit internet access between these networks. This will help ensure that the manufacturing and production network can be isolated and that manufacturing and production operations continue if the corporate network is isolated. Businesses should regularly test contingency plans such as manual controls to ensure that functions that are critical to safety can be maintained during a ransomware attack.

Source: "What We Urge You To Do To Protect Against The Threat of Ransomware," The White House, June 2, 2021, <https://www.iscspo.org/site/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf>

Sotto continued,

“Once a company is made aware of a cyberattack, it must quickly bring in the right experts to assist, including experienced legal counsel, a forensic investigation firm, a ransomware negotiator if hit with ransomware, and an external communications firm, if appropriate under the circumstances. The company would be well advised to coordinate with law enforcement, which often can assist in providing indicators of compromise or other information about the threat actor that will help the team expedite recovery.”¹⁹

The bottom line is that there is much that IT, compliance and financial crime specialists in the private sector can do to address the threat of ransomware and cyberattacks proactively and reactively. One thing is clear: Governments, the private sector and even individuals must work closely together, and across the globe, to avert and address the threat. In other words, there is a lot we can learn from *WarGames*.

Beyond ransomware: Terrorist financing and programmatic money laundering

While ransomware has garnered the most headlines lately, other threats have also moved online. On July 1, 2021, the Israeli National Bureau of Counterterrorism Finance (NBCF), released a copy of an administrative seizure for Bitcoin, Doge, Tron and other cryptocurrency addresses controlled by agents of Hamas.²⁰ The Israeli seizure came less than a year after DOJ announced that IRS-Criminal Investigations, Homeland Security Investigations and the FBI successfully seized over 150 cryptocurrency accounts that laundered funds to and from accounts attributed to the al-Qassam Brigades, Hamas’ military wing.²¹

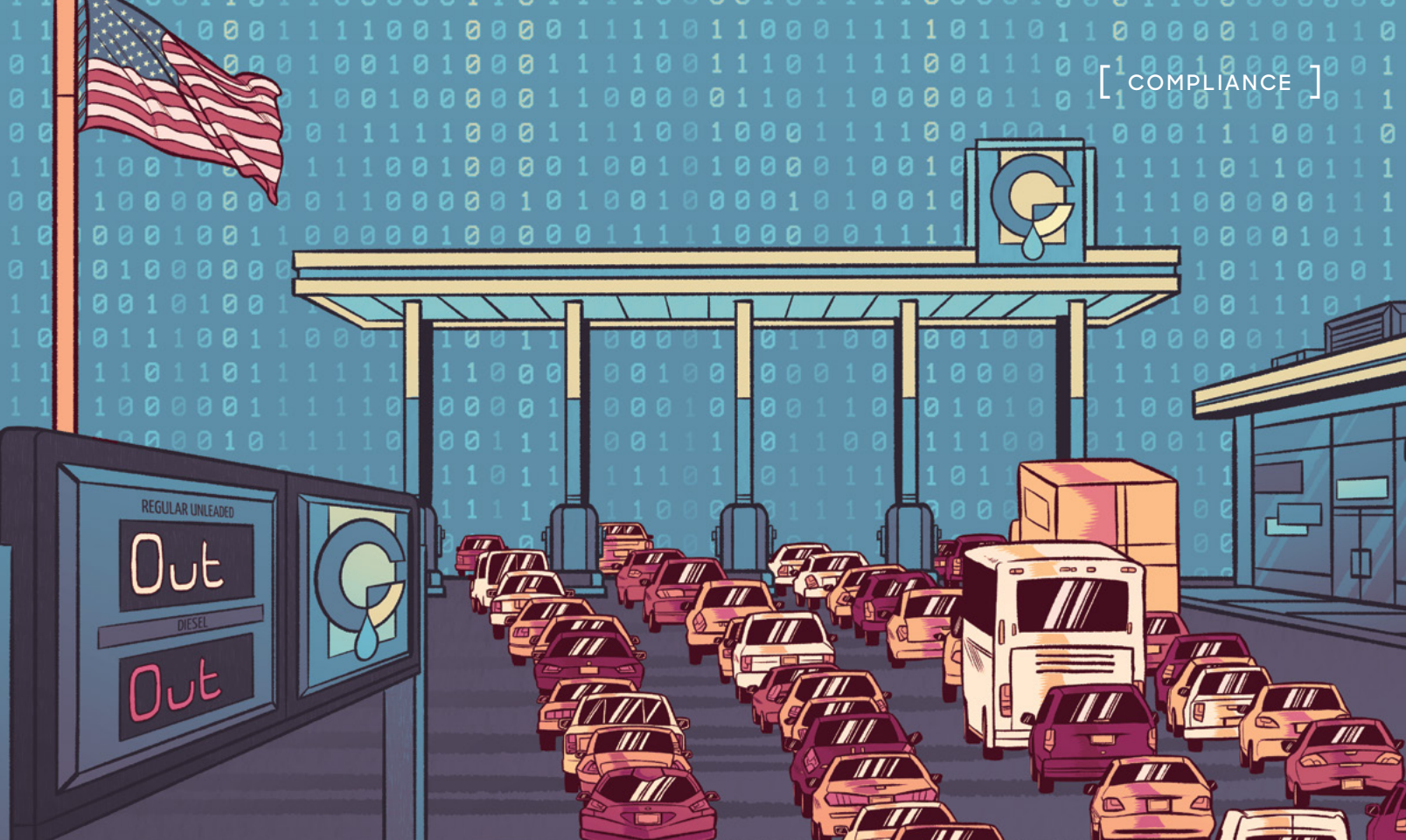
In February 2021, the DOJ unsealed a 33-page federal indictment charging three North Korean computer programmers who, according to the indictment, participated in a wide ranging global criminal conspiracy to conduct a series of malicious cyberattacks resulting in the theft of an unprecedented \$1.3 billion in crypto and fiat currency from financial institutions and other companies worldwide.²² The indictment is riddled with references to malware, initial coin offering scams and phishing attacks aimed at cryptocurrency businesses. Perhaps more concerning than the conduct itself is the professionalism and military precision of North Korean hacking team Lazarus Group, which developed malicious cryptocurrency applications in order to gain backdoor access to their victim’s computer systems.

The bottom line is that there is much that IT, compliance and financial crime specialists in the private sector can do to address the threat of ransomware and cyberattacks proactively and reactively

While RaaS providers, terrorist financiers and nation state-sponsored cybercriminals move to the digital battlefield, so has law enforcement. As seen from the Colonial Pipeline seizure, the identification of Hamas-associated crypto addresses by Israeli authorities and the charges against North Korean cybercriminals, law enforcement is able to use the power and promise of cryptocurrency—the fact that it lives and moves on an open ledger—to track, trace and ultimately recover stolen funds. As the Valjean-and-Javert-style cat and mouse game between law enforcement and illicit actors moves online, it is clear that both the threats and the responses are moving at the speed of the internet. 

*Ari Redbord, head of legal and government affairs, TRM Labs Washington, D.C.
ari@trmlabs.com, Twitter: @ARedbord*

- ¹ Mike Isaac and Sheera Frankel, “Facebook Security Breach Exposes Accounts of 50 Million Users,” *The New York Times*, September 28, 2018, <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>
- ² David E. Sanger and Pranshu Verma, “The F.B.I. confirms that DarkSide, a ransomware group, was behind the hack of a major U.S. pipeline.” *The New York Times*, <https://www.nytimes.com/2021/05/10/us/politics/dark-side-hack.html>
- ³ “Press Briefing by Press Secretary Jen Psaki, Homeland Security Advisor and Deputy National Security Advisor Dr. Elizabeth Sherwood-Randall, and Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger, May 10, 2021,” *The White House*, May 10, 2021, <https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/>
- ⁴ Jordan Robertson and William Turton, “Colonial Pipeline hackers stole data on Thursday,” *Bloomberg*, May 8, 2021, <https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown?sref=SCAzRb9t>
- ⁵ William Turton, Michael Riley and Jennifer Jacobs, “Colonial Pipeline Paid Hackers Nearly \$5 Million in Ransom,” *Bloomberg*, May 13, 2021, <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>



⁶ “Digging into the Darkside Ransomware Payment,” *TRM Labs*, May 14, 2021, <https://www.trmlabs.com/post/darkside-ransomware-report>

⁷ “The moral underground? Ransomware operators retreat after Colonial Pipeline hack,” *Intel 471*, May 14, 2021, <https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime>

⁸ “Darkside Seizure Warrant,” *U.S. District Court for the Northern District of California*, June 7, 2021, <https://www.justice.gov/opa/press-release/file/1402051/download>

⁹ “DAG Monaco Delivers Remarks at Press Conference on Darkside Attack on Colonial Pipeline,” *The United States Department of Justice*, June 7, 2021, <https://www.justice.gov/opa/speech/dag-monaco-delivers-remarks-press-conference-darkside-attack-colonial-pipeline>

¹⁰ “Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,” *The United States Department of Justice*, June 7, 2021, <https://www.justice.gov/opa/pr/departement-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>

¹¹ *Ibid.*

¹² Nicole Perlroth, Erin Griffith and Katie Benner, “Pipeline Investigation Unpicks Idea That Bitcoin Is Untraceable,” *The New York Times*, June 9, 2021, <https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html>

¹³ Aruna Viswanatha and Dustin Volz, “FBI Director Compares Ransomware Challenge to 9/11,” *The Wall Street Journal*, June 4, 2021, <https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003>

¹⁴ “Guidance Regarding Investigations and Cases Related to Ransomware and Digital,” *U.S. Department of Justice Office of the Deputy Attorney General*, June 3, 2021, <https://www.justice.gov/dag/page/file/1401231/download>

¹⁵ Fred Kaplan, “‘WarGames’ and Cybersecurity’s Debt to a Hollywood Hack,” *The New York Times*, February 19, 2016, <https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html>

¹⁶ “The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China,” *The White House*, July 19, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/>

¹⁷ “What We Urge You To Do To Protect Against The Threat of Ransomware,” *The White House*, June 2, 2021, <https://www.iscspo.org/site/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf>

¹⁸ Joseph Johnson, “Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020,” *Statista*, February 16, 2021, <https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/>

¹⁹ Jason Remillard, “Lisa Sotto of Hunton Andrews Kurth: ‘Relationships are incredibly important,’” *ThriveGlobal*, July 30, 2021, <https://thriveglobal.com/stories/lisa-sotto-of-hunton-andrews-kurth-relationships-are-incredibly-important/>

²⁰ “Seizures of Cryptocurrency,” *National Bureau for Counter Terror Financing of Israel*, <https://nbctf.mod.gov.il/en/seizures/Pages/Blockchain1.aspx>

²¹ “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns,” *The United States Department of Justice*, August 13, 2020, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>

²² “Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe: Indictment,” *United States District Court for the Central District of California*, <https://www.justice.gov/opa/press-release/file/1367701/download>



September 11: The 20-year journey

Certain events are etched in our minds forever. For those of us who were working in the public or private sector on September 11, 2001, the attacks against the U.S. by al-Qaeda (al-Qaida) were clearly one of those historic moments that remain embedded in our minds. For those of us who began our careers subsequent to that fateful day, the 20th anniversary of 9/11 is a somber time to take a step back and gain perspective.

September 11, 2001, began as a peaceful and beautiful day on the East Coast of the U.S. At 8:00 a.m. EST, people were going about their daily routine clueless about the catastrophe that was minutes from unfolding on four planes at airports in Boston, Newark and in Northern Virginia. At 8:19 a.m., the first hint of a problem came when flight attendants on one of those planes notified the airline that their flight had been hijacked. At 8:46 a.m., that plane crashed into the North Tower of the World Trade Center. Initially, most people believed it was a tragic accident. Then, at 9:03 a.m., a second plane crashed into the South Tower of the World Trade Center. At that point, a sense of numbness set in with the realization that this was no accident. It was a moment in time that will never be forgotten. The shock was further amplified at 9:37 a.m. when a third plane crashed into the Pentagon. The horror was intensified for the next half hour with the reporting of a fourth plane being hijacked and heading toward Washington, D.C. At 10:03 a.m., because of the heroic action of passengers on board, that flight suddenly crashed in a field in Shanksville, Pennsylvania.

What we knew and what we learned

What we knew was that al-Qaeda was a terrorist organization operating in Afghanistan under the protection of the Taliban. Its leader Osama bin Laden had an intense hatred for the U.S. There were numerous warning signs about bin Laden's aspirations and intent to attack U.S. interests around the world. Unfortunately, as a nation, the U.S. had a false sense of security and invincibility against an international terrorist attack to the homeland.


What we learned in a humbling fashion was how vulnerable an open society like the U.S. is to terrorism. We also learned how adept and adaptive al-Qaeda was at identifying and exploiting systemic vulnerabilities. Conversely, during the immediate investigative response to the 9/11 attacks, the U.S. quickly determined that al-Qaeda and, more broadly, terrorists had two major vulnerabilities: communications and finance. Within weeks after the attacks, the FBI established a communications and financial timeline to trace the origin of the attacks to al-Qaeda.

In the aftermath of the 9/11 attacks, the U.S. Congress established the 9/11 Commission. Their findings were published in the "9/11 Commission Report." This report was the most authoritative, comprehensive, objective and reliable account addressing 9/11. It set forth in great detail how al-Qaeda planned and successfully executed the attack; the vulnerabilities, shortcomings and failures of the U.S. government that offered al-Qaeda the opportunity to succeed; and the countermeasures taken by the U.S. in response. Importantly, the report provided 41 recommendations for the government to adopt to establish best practices and minimize future threats.

The 9/11 Commission issued a report card regarding the progress being made by the U.S. government responding to terrorism. The highest grade, A-, was for the response to terrorist financing. An underlying reason for this was the level of cooperation and partnership the interagency community developed in the form of a working group known as the Policy Coordinating Committee for Terrorist Financing, coupled with what the 9/11 Commission "Monograph on Terrorist Financing" described as "extraordinary cooperation" with the financial community.

Pre-9/11 threat environment

With a false sense of national security, the U.S. government considered counterterrorism a low priority. Consequently, there was a lack of dedicated government resources; a lack of adequate human intelligence; minimal and inconsistent terrorist financing investigations; and ineffective sanctions. These shortcomings were exacerbated by a lack of information sharing between U.S. law enforcement and intelligence agencies. From a financial intelligence perspective, there was a need for more robust Bank Secrecy Act (BSA) regulations and reporting.



Warning signs for the 9/11 terrorist attack originated with the first World Trade Center bombing in February 1993. A massive truck bomb was detonated in the parking garage under the Twin Towers. The intent of that bombing was to cause the Towers to collapse. Although there were serious damages and fatalities, the attack did not achieve the desired results. The mastermind for this attack was Ramzi Yousef. He was the nephew of Khalid Sheikh Mohammed (KSM), who, in turn, was the mastermind for 9/11.

From 1993 to 2001, there were numerous other warning signs. In 1994, Yousef and KSM developed the Manila Air or Bojinka plot in the Philippines. This plot was intended to detonate bombs simultaneously in a series of flights from Asia to the U.S. The Philippine police disrupted the scheme. In 1996 and 1998, bin Laden issued fatwas, a form of a ruling or order, against the U.S. The first fatwa called for Muslims to kill U.S. soldiers; the second called to kill Americans. Al-Qaeda bombed two U.S. Embassies in East Africa in 1998 and the USS Cole in 2000. Mixed in with these activities was fragmented periodic intelligence reporting about likely terrorist attacks in the U.S.

Prior to 9/11, terrorist financing was not a priority for the intelligence community. Likewise, law enforcement, particularly the FBI, did not systemically address terrorist financing. Yet, CIA intelligence reporting before 9/11 advised that al-Qaeda's cash flow during this time was steady and secure.

9/11 attacks

In 1996, KSM met with bin Laden in Tora Bora to propose an operation to attack the U.S. KSM's Tora Bora proposal involved hijacking 10 planes, in the U.S., to attack targets on both the East and West Coasts. KSM's plan was too grandiose, and bin Laden turned it down. Subsequently, in early 1999, bin Laden met with KSM in Kandahar, Afghanistan. At this meeting, bin Laden approved KSM's plan to hijack large commercial planes and use them as missiles to attack targets in the U.S. Shortly thereafter, a series of meetings were held involving bin Laden, KSM and Mohammad Atef, al-Qaeda's military chief and top advisor to bin Laden. At these meetings, plans for the 9/11 attacks were developed, including initial target selection. Although the seed for the 9/11 attacks was planted in 1993, the plot was not conceived until 1999. The combination of bin Laden's organizational leadership and commitment of al-Qaeda resources in the form of funding and operatives with KSM's planning and operational leadership made the plot viable.

The core participants in the 9/11 plot fall into three general roles: the leaders, the facilitators and the 19 hijackers, which can be broken into two smaller groups of the four pilots and 15 muscle hijackers. Beginning in spring 1999, bin Laden, Atef and KSM selected the facilitators and hijackers. The first two hijackers arrived in the U.S. in January 2000. Initially, they were selected as pilots but were unable to acclimate to Western culture. They became muscle hijackers. Subsequently, the four pilots who were more familiar with Western society were chosen. They entered the U.S. in the spring and summer of 2000. The pilots spent the coming year in flight training and conducting in-flight surveillances on cross-country aircraft to identify points of vulnerability for hijacking planes. The 13 remaining muscle hijackers entered the U.S. in the spring and summer of 2001. In the days leading up to the attacks, the 19 hijackers formed the four flight teams. On the morning of 9/11, the hijackers successfully executed their plan.

One point concerning the 9/11 attacks is irrefutable. The plot required funding. The cost was between \$400,000 and \$500,000. Approximately \$326,000 passed through financial institutions. Bin Laden provided most of the funding for the 9/11 plot to KSM, who then provided the money directly to the hijackers or indirectly through three facilitators. Each of the 19 hijackers opened bank accounts in the U.S. to deposit and withdraw money in order to support them in furtherance of the plot. Foreign bank accounts were also used, as well as money services businesses (MSBs) and foreign exchanges. Approximately 20 wire transfers were sent between the facilitators and the hijackers, which included unused funds the hijackers wired back to facilitators.




Immediately following the attacks, the FBI initiated an investigation. Based on cell phone calls from each hijacked flight, the 19 hijackers were quickly identified and the financial trail began to unfold. It started with the manner in which hijackers purchased airline tickets, the identification of bank accounts, tracking the wire transfers, and then establishing and building the timeline of bank transactional activity and communications. The responsiveness of the financial services industry greatly facilitated this process.

Post-9/11 impact

Nearly 3,000 people were killed in the attacks. In the years since that tragic day, hundreds of first responders have died from toxins they were exposed to at all four crash sites. Secondary multifaceted impacts of 9/11 included the exposed systemic intelligence failures, level of complacency, lack of information sharing, limited focus on terrorist financing, need for stronger BSA reporting requirements and the need for more robust public-public and public-private partnerships. All of these vulnerabilities were successfully exploited by al-Qaeda.





The U.S. government launched an urgent and massive response to 9/11, which began to fuse the existing systemic failures exposed by the terrorist attacks. There was a military response; intelligence and investigative response; regulatory and sanctions response; and the development of sustainable public-public and public-private partnerships. In addition, the international community, including the United Nations, rallied to support the U.S. and broadly took measures to criminalize terrorism and terrorist financing.

Notable countermeasures were established in the aftermath of 9/11 on many levels. They have been built upon and enhanced in the years since, with the objective to minimize the risk of future 9/11-like attacks. In addition to the formation of the 9/11 Commission, in October 2001, the U.S. Congress passed the USA PATRIOT Act, strengthening legal provisions to deal with the threat of terrorism. The financial provisions of the USA PATRIOT Act greatly enhanced BSA requirements. The Financial Action Task Force (FATF) held a special plenary session on terrorist financing in Washington, D.C. in October 2001, where they implemented the Special Recommendations on Terrorist Financing. In October 2002, FATF issued typologies and guidance regarding terrorist financing. Since that time, FATF has continued to provide periodic guidance regarding terrorist financing.

Current threat environment

Over the 20 years since 9/11, the terrorist threat environment has continuously evolved. The primary threat between 2001 and early 2019 was organization driven. There was an evolution and devolution of organizations. Preceding 9/11, and especially on and in the aftermath of 9/11, al-Qaeda posed the primary threat. In 2013, with the development of a caliphate in Syria and Iraq, the Islamic State (IS) emerged as the most significant terrorist threat. In 2019, the caliphate fell and IS transformed into an insurgency.


As the U.S. and like-minded countries prioritize the threats posed by HVEs and DVEs, they cannot lose sight of the threat posed by foreign terrorist organizations

With their ability to recruit and radicalize extremists through the internet, al-Qaeda and IS began to transform the threat from organizations to individuals in the form of homegrown violent extremists (HVEs). HVEs are inspired by the ideology of foreign Islamist terrorist groups. Along with the HVE threat, beginning in 2019, the threat of domestic violent extremists (DVEs) became more prevalent. DVEs are individuals who commit violent acts in furtherance of ideological goals stemming from domestic influences, such as racial bias and anti-government sentiment. The top threat from DVEs stems from those identified as racially or ethnically motivated violent extremists (RMVEs).

In 2021, the most significant terrorist threats emanated from HVEs and DVEs. The significance of the DVE threat shockingly manifested itself with the January 6 riot at the U.S. Capitol. As the U.S. and like-minded countries prioritize the threats posed by HVEs and DVEs, they cannot lose sight of the threat posed by foreign terrorist organizations. Although currently lacking the capacity to do so, both al-Qaeda and IS aspire to conduct a 9/11-like attack against the U.S.

From a terrorist financing perspective, the shift from an organizational to individual-centric threat environment, one that is more decentralized and leaderless, means that financing is more localized. Thus, funding is less likely to flow from organizations to operatives as it did for 9/11. Funding is more likely to be self-generated and originate from local sources. Whether attacks are perpetrated by HVEs or DVEs, lone actor attacks require minimal funding. They tend to be cheaper, less sophisticated, smaller scale and more likely to succeed.

Conclusion

It took more than two years to plan and execute the 9/11 attacks. For two years, money was spent preparing for and executing the terrorist attacks of 9/11. For two years, there were touch points with banks and MSBs. Even with two years of touch points, the transactional activity of the hijackers was unremarkable and not suspicious. However, for the most part, the hijackers and their facilitators used their true identities and left a financial trail. That financial trail allowed the FBI to follow the money, link the hijackers and facilitators together, and take the funding directly back to KSM and indirectly to bin Laden. The funding flow for 9/11 was identified in a matter of weeks due to the unprecedented support that the FBI received from the financial sector. As evidenced with the Capitol riot, the threat landscape has changed. The funding requirements have changed from organizational to lone actors or groups of individuals. If best practices have taught us anything, the daunting challenge presented by self-funded terrorists requires sustainable and meaningful public-private partnerships. 

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



Elder financial exploitation: A monumental crisis

First the ingredients: One coronavirus that forces people to isolate in their own homes; add increased reliance on telephones and computers as means of communication; then remove layers of protection by eliminating home visits from Adult Protective Services case workers; insert a measure of desperation from people who have lost their sole source of income because of the pandemic; throw in the factor of an aging society with 10,000 people turning 65 every day; incorporate multiple suspects looking for an easy target to exploit; and finally mix in a whole group of older victims who are either too embarrassed to report or who, because of cognitive impairment, are unaware of what has occurred. This is a perfect recipe for elder financial exploitation, which has been sweeping through this country for years and is now becoming a monumental social and economic crisis in need of an aggressive response.

For 22 years I was privileged to head up the San Diego District Attorney’s Elder Abuse Unit from 1996 to 2018. But as calls kept coming in from all over the U.S. requesting training for local law enforcement, prosecutors and social workers, I decided it was time to pass the baton to a younger prosecutor. That allowed me the opportunity to share my court room experiences prosecuting elder abuse cases with a wider audience.

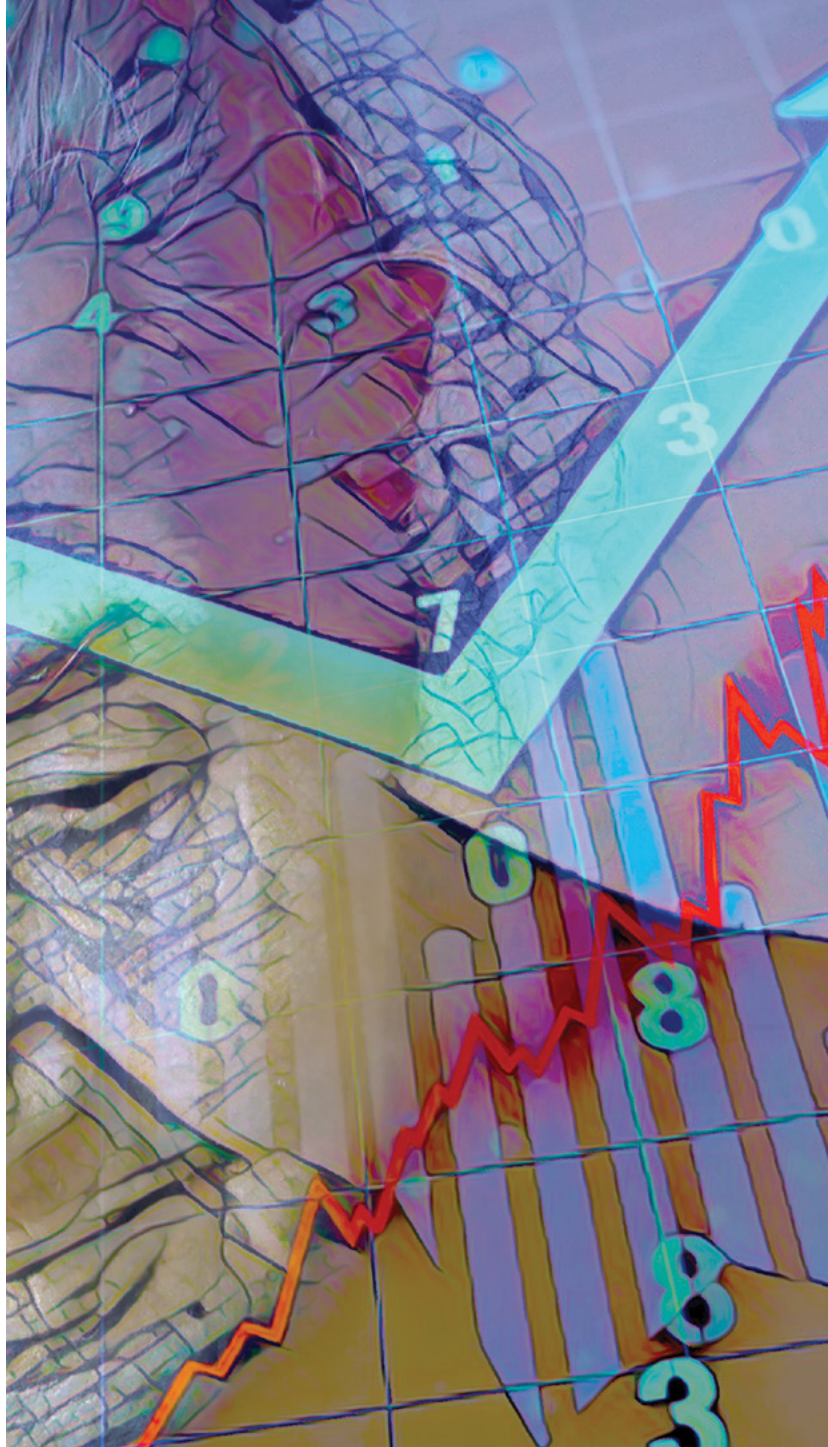
Sixty-five percent of the felony elder abuse cases that I prosecuted involved some form of financial exploitation. Regardless of the type of exploitation—whether it involved cash, real property, investments or personal assets—the challenge was always the same. How do I go about proving that the suspect has taken property from the elderly victim without consent and with the intent to deprive permanently?

Four different scenarios emerged. The first two were straight forward, but the third and fourth were often far less clear cut.

Scenario one involved a victim who was able to testify competently that the defendant had taken property without the victim’s consent.

In scenario two, the victim was unable to testify because of advanced dementia or some other extreme mental impairment. The theft occurred at a time when the victim was already suffering from that condition. After laying an evidentiary foundation showing the transfer of assets, I then relied upon the testimony of a medical treating practitioner who would offer an opinion that the victim lacked the ability to provide consent to the transfer.

In scenario three, the victim was already deceased by the time that the theft was discovered. Traditionally, such a situation would have led to an immediate decision by law enforcement not to investigate the matter further because of an inability to prove that the victim did not give consent. However, I discovered that it might still be possible to prove a case of theft, if in fact, there was medical evidence as outlined in scenario two above, by showing a documented history of incapacity.



Alternatively, if the theft involved forged documents, then we might have been able to establish guilt through a forensic handwriting expert. In addition, if prior to death the victim had made some “excited utterances” demonstrating a lack of consent to the transfer, then we might have been successful in getting such out of court statements admitted as an exception to the hearsay rules.

In scenario four, the victim was marginally competent to testify even though there might have been some indications of memory deficiencies. At first glance it might seem that the victim had voluntarily transferred assets to the defendant, who in turn would typically explain the transfer as a gift or a loan. Again, law enforcement traditionally declined to investigate on the basis that no apparent crime had been committed. The conclusion would often be that the suspect had unduly influenced the victim to part with their property by using clever manipulation rather than force or duress. However, we discovered that such circumstances required an investigation that focused on the following factors:

- How, where and when the victim and suspect met?
- The spending habits of the victim prior to meeting the suspect. If it could be established that the victim had a history of frugality, then it might be possible to highlight the transfer as totally out of character.
- The methods used by the suspect to influence the victim: Did the suspect isolate the victim from family and friends or create a false “identity” that would appeal to the victim? Did the suspect perform certain acts that made the victim increasingly dependent on their relationship?

Being able to identify an exploitation case as fitting into one of the above scenarios certainly aided me in evaluating a case for prosecution. However, getting such a case in front of a judge or jury requires collaboration through an effective multi-disciplinary team approach.

Applying a multi-disciplinary team approach

To succeed in combating this escalating crime of elder financial exploitation—which some have called the crime of the 21st century—it takes a combined effort from multiple agencies. Thankfully, more financial abuse specialist teams (FAST) have been established in various jurisdictions. So, who should be part of this team?

To succeed in combating this escalating crime of elder financial exploitation—which some have called the crime of the 21st century—it takes a combined effort from multiple agencies

Some obvious participants include local law enforcement, the county prosecutor’s office, Adult Protective Services, the long-term care Ombudsman and the Public Guardian. There should also be representatives from the state attorney general’s office and the U.S. attorney’s office along with members of the Postal Inspection Service, Social Security Administration, FBI, probate court investigators and the Contractors State License Board. In addition, fraud investigators from banks, credit unions, investment brokers and other financial institutions are vital members. Moreover, adding a forensic accountant, a geriatric specialist and some local providers of aging services would give the team valuable insight.


Too often reports of suspected elder financial exploitation never reach a court room. Sometimes the response from law enforcement is “it’s just a civil matter,” especially when the suspect brandishes a power of attorney document. Sometimes the victim or the victim’s family is told that “the crime did not occur here” or “the suspect is probably overseas and we will not be able to identify anyone.” And sometimes a prosecutor will discourage any investigation by suggesting that the victim will make an ineffective witness because of age or impairment.

Suspects who commit these crimes of opportunity often rely on the fact that their conduct will survive any scrutiny by law enforcement or prosecutors. And the impact of the pandemic has further emboldened such predators.

Conclusion

In order to rise to the challenge, it is important to recognize “ageism” misconceptions that can hinder, the importance of a team approach and the value of combining various resources to tackle this insidious crime.

Elder financial exploitation is a violent crime. It affects not just the financial security of an older adult, it can impinge upon mental as well as physical health, and it can also cause a dramatic deterioration in lifestyle. Many of the victims are members of “our finest generation.” Surely, they are owed not just gratitude for prior service but also a commitment to pursuing justice on their behalf.

If you are not already a member of an elder abuse task force, maybe you will consider joining one—or if there is not one in your area, would you be willing to start the conversation? 

Paul Greenwood, retired San Diego County deputy district attorney; consultant and trainer, Greenwood Law Corp.



THE NEW WHISTLEBLOWER PROGRAM AML PROFESSIONALS SHOULD KNOW



The Anti-Money Laundering Act of 2020 (AMLA) is the most significant change to the U.S.’ anti-money laundering (AML) laws in more than a decade. One provision of interest to financial institutions (FIs) and AML professionals is the expansion of the Bank Secrecy Act’s (BSA) whistleblower program. Whistleblowers can now anonymously report BSA violations and receive up to 30% of the monetary sanctions the government imposes, which can sometimes total hundreds of millions of dollars. The significant incentives now in place are likely to result in a dramatic increase in whistleblower reports, much like what the U.S. Securities and Exchange Commission (SEC) witnessed following the creation of its separate program in 2010. The BSA requires FIs to implement an effective AML program that detects and reports suspicious transactions.¹ If an FI violates this requirement, it faces penalties between \$25,000 and \$100,000 for each underlying transaction.² While the BSA previously had a program for rewarding the so-called “informants,” the amount of any award was capped at \$150,000.³ In addition, the BSA contained no provision for anonymously disclosing violations.

The AMLA made several important changes to the BSA’s whistleblower program. It significantly increased the potential awards for disclosing BSA violations, added protections against retaliation and created a procedure for anonymous reporting. Now, a “whistleblower” who provides “original information” about violations of the BSA can receive up to 30% of any monetary sanction in excess of \$1 million that the government recovers.⁴

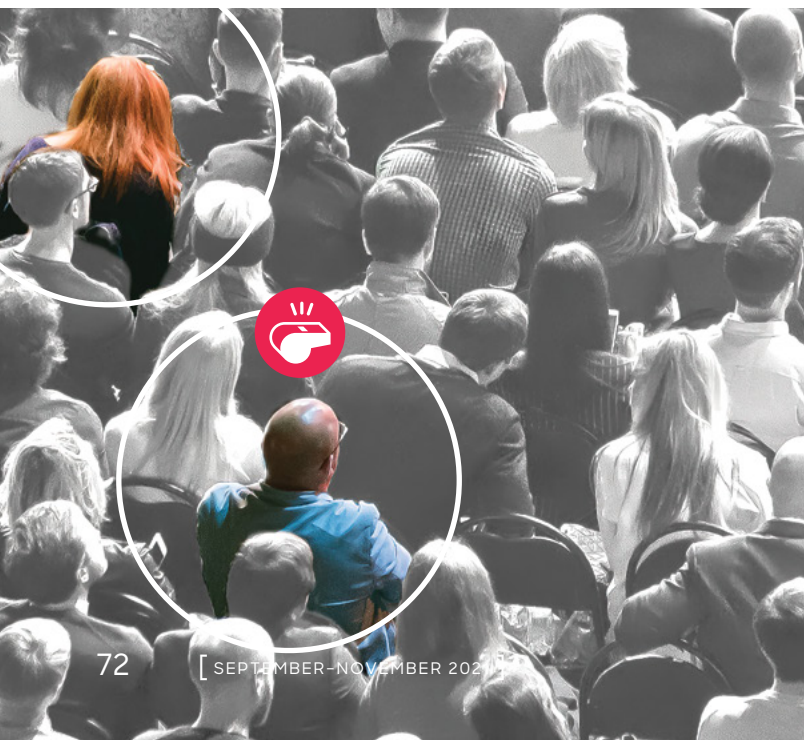
A whistleblower can be “any individual” or group of individuals “acting jointly.”⁵ U.S. citizenship is not required, as money laundering frequently crosses borders. The “original information” that a whistleblower provides can derive from the whistleblower’s independent knowledge or analysis, as long as it is not already known to the government or available in public records.⁶

Whistleblowers also do not need to report the information directly to the government.⁷ Instead, they can relay it to their employers as part of their job duties. The secretary of the treasury has discretion over what amount to award a whistleblower but must consider the significance of the original information to subsequent enforcement actions and the degree of assistance that the whistleblower or the counsel provides in such actions.⁸

The new AML whistleblower program could produce substantial awards as violations of the BSA frequently result in civil and criminal penalties in the hundreds of millions of dollars. For example, in January 2021, the Financial Crimes Enforcement Network (FinCEN) assessed a \$390 million civil money penalty against Capital One, National Association.⁹ That penalty resulted from Capital One’s failure to implement effective AML controls at a check-cashing subsidiary. Capital One’s AML deficiencies led it to not file suspicious activity reports on transactions by check-cashing outlets that later pleaded guilty to loan sharking, illegal gambling, tax evasion and money laundering, among other crimes.

Similarly, in 2018, U.S. Bank paid \$528 million in penalties under a deferred prosecution agreement with the U.S. Attorney’s Office for the Southern District of New York.¹⁰ Among other things, the government faulted U.S. Bank for employing an inadequate number of AML personnel, stretching them “dangerously thin” and limiting the number of potentially suspicious transactions it would review. Following the AMLA, penalties like those against Capital One and U.S. Bank could give rise to awards of over \$100 million for any whistleblower who provided original information.

The AMLA also creates significant protections against retaliation.¹¹ It prohibits an employer from discharging, demoting, suspending, blacklisting or discriminating “in any other manner” against whistleblowers who disclose conduct that they reasonably believe violates the AML law. That prohibition applies even if the conduct is



**THE NEW AML WHISTLEBLOWER PROGRAM
COULD PRODUCE SUBSTANTIAL AWARDS AS
VIOLATIONS OF THE BSA FREQUENTLY RESULT IN
CIVIL AND CRIMINAL PENALTIES IN THE
HUNDREDS OF MILLIONS OF DOLLARS**



THE AMLA PERMITS WHISTLEBLOWERS TO REPORT INFORMATION “ANONYMOUSLY” THROUGH A COUNSEL


disclosed to the whistleblower’s supervisors, rather than the government. A whistleblower who suffers discrimination can file a complaint with the secretary of labor. If the secretary of labor does not issue a final decision within 180 days, the whistleblower can sue in federal court. The potential remedies include reinstatement, double the amount of any back pay owed and other compensatory damages, including attorneys’ fees.

Finally, the AMLA permits whistleblowers to report information “anonymously” through a counsel.¹² Under this approach, the government receives only the counsel’s name and contact information, and any follow-up inquiries are relayed to the whistleblower through the counsel. Before receiving any award, whistleblowers must disclose their identities. This is required because certain groups, such as government employees, are excluded from receiving whistleblower awards.¹³ However, when a whistleblower’s identity is disclosed, the AMLA requires the government to treat that information confidentially and places specific limitations on disclosure including the limitations in the Privacy Act.

The AMLA is likely to increase the number of whistleblower reports received by AML enforcement agencies dramatically. The provisions described above are highly similar to the SEC’s whistleblower program created by the Dodd-Frank Act in 2010. Since that program’s enactment, the number of whistleblower tips received by the SEC has increased each year, and now totals more than 40,000. Between 2012 and 2020, the SEC paid \$562 million in whistleblower awards.¹⁴

The AMLA’s expansion of the BSA whistleblower program has significant implications for both AML professionals and FIs. AML professionals with knowledge of BSA violations have much stronger incentives to disclose what they know to the government, and now they can do so anonymously. These incentives will likely lead to many reports as the history of the SEC’s program demonstrates.

This new reality also creates risks for FIs, even if they are in full compliance with the BSA. A whistleblower report that lacks foundation can still result in an investigation, and FIs targeted by such investigations will need to devote significant resources to responding. FIs can mitigate the risk of an unexpected investigation by taking several measures to encourage internal reporting. The first step is the implementation of internal reporting mechanisms such as anonymous hotlines. But reporting mechanisms alone are not enough. Employees must believe that their institution will take such complaints seriously and not engage in retaliation. The institution can cultivate that belief by encouraging reporting at the highest levels, enacting robust anti-retaliation protections and making investigations into complaints as transparent as possible. Reporting programs that employees regard as credible maximize an institution’s opportunity to resolve issues proactively rather than in response to an investigation. The AMLA encourages internal reporting by including internal whistleblowers among those eligible for an award.

AML professionals and FIs with questions or concerns about the new whistleblower program would be well-advised to consult with a counsel. While the AMLA has set forth the program’s boundaries, many aspects of the program’s future will depend on enforcement agencies and the regulations or other guidance they issue. Experienced counsel can help professionals and institutions keep up with new developments, analyze their implications and plot an effective course of action. 

*Caleb Hayes-Deats, counsel,
MoloLamken LLP, D.C., USA, chayes-deats@mololamken.com¹⁵*

¹ 31 U.S.C. §5318.

² *Id.* §5321.

³ 31 U.S.C. §5323(b) (2020).

⁴ 31 U.S.C. §5323(b)(1). Monetary sanctions include “penalties, disgorgement, and interest,” but not “forfeiture,” “restitution,” or other “victim compensation.” *Id.* §5323(a)(2).

⁵ *Id.* §5323(a)(5).

⁶ *Id.* §5323(a)(3).

⁷ *Id.* §5323(a)(5).

⁸ *Id.* §5323(c)(1).

⁹ “Assessment of Civil Monetary Penalty Number 2010-01,” *Financial Crimes Enforcement Network*, https://www.fincen.gov/sites/default/files/enforcement_action/2021-01-15/Assessment_CONA%20508_0.pdf

¹⁰ “Manhattan U.S. Attorney Announces Criminal Charges Against U.S. Bancorp For Violations Of The Bank Secrecy Act,” *The United States Attorney’s Office Southern District of New York*, February 15, 2018, <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-us-bancorp-violations-bank>

¹¹ 31 U.S.C. §5323(g).

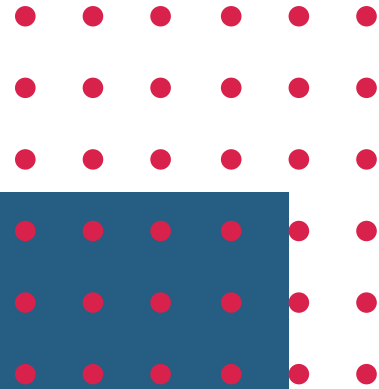
¹² 31 U.S.C. §5323(d).

¹³ 31 U.S.C. §5323(c)(2).

¹⁴ “2020 Annual Report to Congress Whistleblower Program,” *U.S. Securities and Exchange Commission*, https://www.sec.gov/files/2020%20Annual%20Report_0.pdf

¹⁵ Hayes-Deats previously worked at the U.S. Attorney’s Office for the Southern District of New York and was involved in FinCEN’s assessment of AML penalties against U.S. Bank. The views expressed in this article are his alone.





The European cybersecurity ecosystem: A war on cybercrime

On June 23, the European Commission announced a proposal to establish a Joint Cyber Unit in response to large-scale security incidents¹ related to cybercrime.

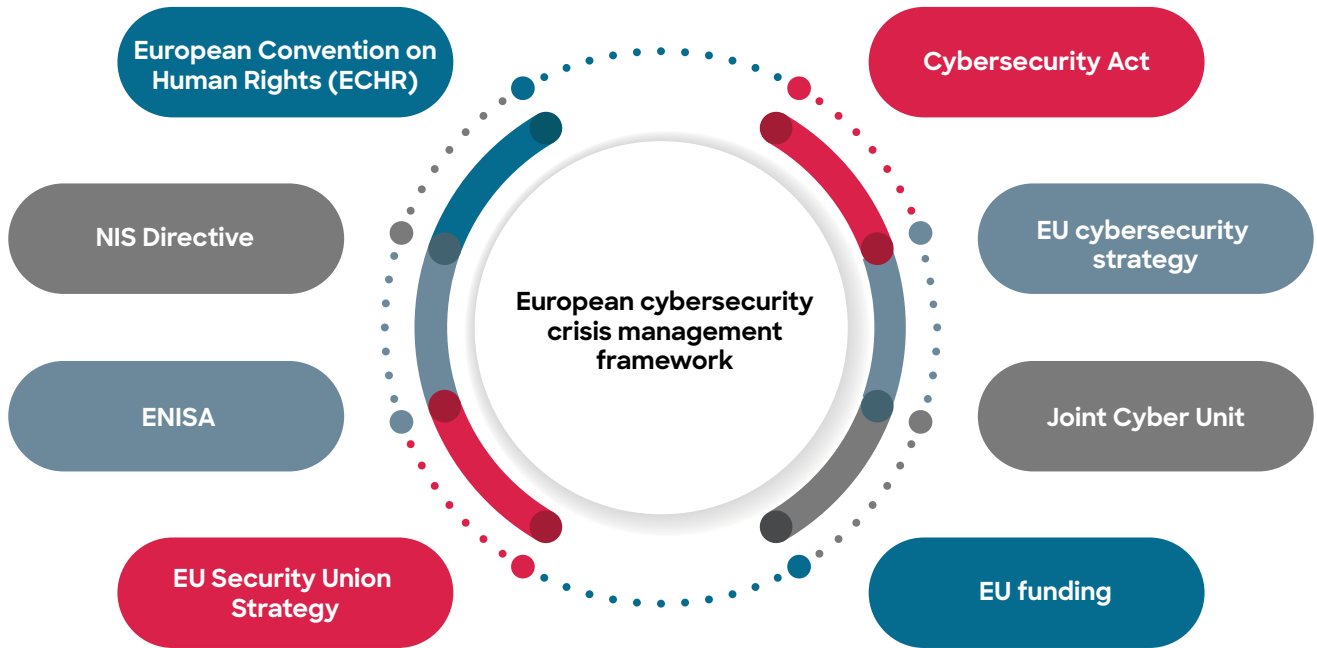
The proposal is part of a vast and seemingly endless array of proposals, guidelines, strategies and legislation by the European Union (EU) and the European Commission to combat cybercrime. This is not deliberate but rather indicative of the nature of cybercrime. The internet of things² has now become the reality of internet infrastructure globally, resulting in a borderless and virtual space where cybercriminals can attack any industry or individual from anywhere in the globe.

The EU is currently constituted by 27 countries. Therefore, effectively combating and prosecuting cybercrime is reliant on synchronizing the legal, cultural and constitutional dispensations of every country in the EU.

From a prosecutorial perspective, the search and seizure of electronic evidence is the centerpiece in fighting cybercrime. National laws must conform not only with regards to search and seizure law, they must also be within an accepted human rights dispensation, which is provided by the European Convention on Human Rights (ECHR).

As a consequence of these complexities, the EU has developed an intricate “ecosystem” in which EU members can effectively combat cybercrime (see Figure 1).

Figure 1: The European cybersecurity crisis management framework



The ecosystem: The European cybersecurity crisis management framework

Search and seizure legislation and the ECHR

The ECHR has become the watchdog and the standard for all search and seizure legislation (along with other human rights interests) in the EU. The ECHR's principles are enforced by the European Court of Human Rights (ECtHR).

The ECHR applies to the 47 member states of the Council of Europe³ and was established and signed in Rome on November 4, 1950. It came into force on September 3, 1953, when it was adopted by the Assembly of the Council of Europe.⁴

State parties to the convention are bound by the decision of the court and the court is empowered to hear not only interstate but also individual petitions or complaints without the prior approval of local governments.⁵

The ECHR has become the watchdog and the standard for all search and seizure legislation (along with other human rights interests) in the EU



The European Union Agency for Network and Information Security

The European Union Agency for Network and Information Security (ENISA) was founded in 2004 with the purpose of achieving “a high common level of cybersecurity across Europe.”⁶ ENISA is part of the EU’s–coordinated response to cybercrime incidents, crises management and it assists the European Commission when necessary.⁷ This is done within another “framework” called the Integrated Political Crisis Response (IPCR).⁸ ENISA, in conjunction with member states, develops “EU-level cyber crisis management procedures to improve situational awareness in the event of cross-border cyber incidents, to assist both national level and EU-level decision makers in taking the right decisions.”⁹

Cybersecurity Act

ENISA’s regulation is Regulation (EU) 2019/881,¹⁰ known as the Cybersecurity Act. The Cybersecurity Act establishes a cybersecurity certification framework for products and services.¹¹ The act strengthens ENISA’s mandate to support member states with tackling cybersecurity threats and attacks. It also directs ENISA to support member states in establishing an EU-wide cybersecurity certification framework in which it will play a key role.¹²

NIS Directive and NIS2

Published in 2016, the NIS Directive (EU 2016/1148)¹³ is part and parcel of “The EU’s Cybersecurity Strategy for the Digital Decade” and the first piece of an EU-wide cybersecurity legislation. The directive describes national frameworks on the security of network and information systems that need to be adopted by member states.¹⁴



The NIS Directive is divided into the following three parts:¹⁵

- “1. National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g., they must have a national CSIRT, perform cyber exercises, etc.
2. Cross-border collaboration: Cross-border collaboration between EU countries, e.g., the operational EU CSIRT network, the strategic NIS cooperation group, etc.
3. National supervision of critical sectors: EU Member States have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online marketplaces, cloud and online search engines)”¹⁶

The goal of the directive “is to enhance cybersecurity across the EU”¹⁷ and because it is an EU directive, every member state has started to adopt it.

The European Commission is required by article 23 of the directive to review the functioning of the directive periodically. As a result of the review process, NIS2 was presented to the EU on December 16, 2020.¹⁸ NIS2 repeals the current NIS Directive. NIS2 is said to modernize the existing legal framework “taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape.”¹⁹

The EU cybersecurity strategy

The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU cybersecurity strategy on December 16, 2020.²⁰ The EU’s cybersecurity strategy “describes how the EU can harness and strengthen all its tools and resources to be technologically sovereign.”²¹ It is a tool of general application and has described “three principal instruments” for “deployment” namely, regulatory, investment and policy initiatives. These three instruments will address the following:

- “Resilience, technological sovereignty and leadership
- Operational capacity to prevent, deter and respond
- Cooperation to advance a global and open cyberspace”²²

A number of initiatives, such as the Joint Cyber Unit, form part of the EU’s cybersecurity strategy.

EU Security Union Strategy: “Connecting the dots in a new security ecosystem”

On July 24, 2020, the European Commission set out a new EU Security Union Strategy for 2020 through 2025. As with the EU’s cybersecurity strategy, the EU Security Union Strategy is a tool of general application that sets out principles or in its case “4 strategic priorities” that must be implemented at the EU level as part of its strategy.²³



The Joint Cyber Unit is aimed at bringing together all the EU’s resources and expertise to prevent, deter and respond to mass cyber incidents and crises

The four strategic priorities are listed below:²⁴

- A future-proof security environment
- Tackling evolving threats
- Protecting Europeans from terrorism and organized crime
- A strong European security ecosystem

Figure 2 describes these four strategic priorities in more detail.

Joint Cyber Unit

On June 23, the European Commission proposed to build a new Joint Cyber Unit to “tackle the rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union.”²⁵

The Joint Cyber Unit is aimed at bringing together all the EU’s resources and expertise to prevent, deter and respond to mass cyber incidents and crises. The unit is also a deliverable of the EU cybersecurity strategy and the EU Security Union Strategy.²⁶

Figure 2: The EU Security Union Strategy



Source: "EU Security Union Strategy: connecting the dots in a new security ecosystem," European Commission, July 24, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

EU funding

The EU cybersecurity strategy will purportedly receive "an unprecedented level of investment"²⁷ over the next seven years. The investment will be provided for in the 2022 long-term EU budget. The mechanisms through which the long-term EU budget will be affected are the Digital Europe Programme,²⁸ Horizon Europe²⁹ and the Recovery Plan for Europe.³⁰ Further to the long-term EU budget, an objective has been set to reach up to 4.5 billion euros (\$5.3 billion) through combined investment from the EU, the member states and the industry.³¹ The Cybersecurity Competence Centre and Network of Coordination Centres³² will be utilized in achieving this goal and ensuring that a major portion of the funds gets to small and medium-sized enterprises.

The impact of the European cybersecurity ecosystem and current state of affairs

At this stage, the ecosystem is very much just an idea. It consists of proposals rather than actual institutions and can be described as a forward-looking cybersecurity framework rather than an existing one.

The funding for the cybersecurity strategy will only commence in 2022 and the Joint Cyber Unit is a European Commission proposal that still must be implemented. Therefore, it is clear there has been no impact on cybercrime with regards the new ecosystem.

What is the current state of affairs in regard to combating cybercrime in the EU? ENISA has been part and parcel of combating cybercrime in the EU since 2004 and the NIS Directive was published in 2016.

The impact of this forward-looking cybersecurity framework will be felt in a few years. The funding starts in 2022 and it is doubtful that any of its proposals will become actionable before 2023. The Commission has slated the opening of the operational phase of Joint Cyber Unit for June 30, 2022, and for the unit to be fully established on June 30, 2023.³³

The European Commission's website states the following, "The EU cybersecurity ecosystem is wide and varied and through the Joint Cyber Unit, there will be a common space to work together across different communities and fields, which will enable the existing networks to tap their full potential. It builds on the work started in 2017...."³⁴

In conclusion, the European cybersecurity ecosystem looks to be a great implementable strategy that seems to have all the necessary ingredients to succeed; namely, funding, member cooperation, as well as the necessary skillsets and expertise. **A**

Gideon Bouwer, information technology law attorney, Cyberlawforensics, South Africa, gideon@cyberlawforensics.co.za

¹ “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents,” *European Commission*, June 23, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088

² “What is IoT?” *Oracle*, <https://www.oracle.com/za/internet-of-things/what-is-iot/>. “The Internet of Things (IoT) describes the network of physical objects—‘things’—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.”

³ The Council of Europe was established in 1949 and has 47 European states as its members.

⁴ Dietrich Schindler, “European Convention on Human Rights in Practice,” *Washington University Law Quarterly*, January 1962, https://openscholarship.wustl.edu/law_lawreview/vol1962/iss2/2

⁵ “European Convention on Human Rights: Europe [1950].” *Encyclopedia Britannica*, November 4, 1950, <https://www.britannica.com/event/European-Convention-on-Human-Rights-Europe-1950> (accessed September 17, 2020).

⁶ “About ENISA - The European Union Agency for Cybersecurity,” *European Union Agency for Cybersecurity*, <https://www.enisa.europa.eu/about-enisa>

⁷ “EU-level Cyber Crisis Management,” *European Union Agency for Cybersecurity*, <https://www.enisa.europa.eu/topics/cyber-crisis-management/eu-cooperation>

⁸ “How does the Integrated Political Crisis Response (IPCR) mechanism work?” *Council of the European Union*, 2018, <https://www.consilium.europa.eu/en/documents-publications/publications/ipcr/>. “The IPCR is the Council’s crisis response mechanism; a ‘tool’ in the hands of the Presidency to coordinate the political response to major cross sectoral and complex crises, including acts of terrorism.”

⁹ “EU-level Cyber Crisis Management,” *European Union Agency for Cybersecurity*, <https://www.enisa.europa.eu/topics/cyber-crisis-management/eu-cooperation>

¹⁰ “ENISA Mandate and Regulatory Framework,” *European Union Agency for Cybersecurity*, <https://www.enisa.europa.eu/about-enisa/regulatory-framework>

¹¹ “The EU Cybersecurity Act,” *European Commission*, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

¹² “The EU Cybersecurity Act is Now Applicable,” *Jones Day*, June 2019, <https://www.jonesday.com/en/insights/2019/06/the-eu-cybersecurity-act-is-now-applicable>

¹³ “NIS Directive,” *European Union Agency for Cybersecurity*, <https://www.enisa.europa.eu/topics/nis-directive>

¹⁴ Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert. “The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation,” *Computer Law & Security Review*, 35, no. 6, November 2019, <https://www.sciencedirect.com/science/article/pii/S0267364919300512> (accessed 11 August 2021).

¹⁵ “NIS Directive,” *European Union Agency for Cybersecurity*, <https://www.enisa.europa.eu/topics/nis-directive>

¹⁶ *Ibid.*

¹⁷ *Ibid.*

¹⁸ “NIS Directive,” *European Commission*, <https://digital-strategy.ec.europa.eu/en/policies/nis-directive>

¹⁹ *Ibid.*

²⁰ “The EU’s Cybersecurity Strategy for the Digital Decade,” *European Commission*, December 16, 2020, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

²¹ “The Cybersecurity Strategy,” *European Commission*, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

²² *Ibid.*

²³ “EU Security Union Strategy: connecting the dots in a new security ecosystem,” *European Commission*, July 24, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

²⁴ *Ibid.*

²⁵ “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents,” *European Commission*, June 23, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088

²⁶ *Ibid.*

²⁷ “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient,” *European Commission*, December 16, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

²⁸ “Commission welcomes political agreement on €7.5 billion Digital Europe Programme,” *European Commission*, December 14, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2406

²⁹ “Commission welcomes political agreement on Horizon Europe, the next EU research and innovation programme,” *European Commission*, December 10, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2345

³⁰ “Recovery plan for Europe,” *European Commission*, https://ec.europa.eu/info/strategy/recovery-plan-europe_en

³¹ “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient,” *European Commission*, December 16, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (accessed August 11, 2021).

³² “Commission welcomes political agreement on the Cybersecurity Competence Centre and Network,” *European Commission*, December 11, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384

³³ *Ibid.*

³⁴ “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents,” *European Commission*, June 23, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088





Become a Certified Specialist with a Global Certification in AML or Sanctions Compliance



The Gold Standard
in AML certifications
worldwide



Understanding
and interpreting
changing sanctions
regimes



Start your journey at
www.acams.org

Analyzing South Korea's 'Nth Room' case

In 2020, the global lockdown saw an increased supply and demand of online child sexual abuse material (CSAM) accessed through social media, instant messengers, chatrooms and online games by users looking to exchange and offer illicit content and to quote Europol, “exploit isolation.”

Of particular concern is that the illicit content is being largely self-generated by underage victims and obtained through coercion as criminals tap into a broader scope of participants and survivors.¹ An example of the latest twist in child and underage sexual exploitation is the South Korean case referred to as the “Nth Room” case.

The following analysis of the Nth Room case creates awareness of these crimes and provides anti-financial crime professionals with the knowledge to identify, flag and report them. It also provides law enforcement and prosecutors with the tools and knowledge to assist in the arrest and prosecution of criminals engaged with CSAM.

CSAM's constantly evolving nature makes it difficult to prevent, identify, track, trace and report

CSAM's constantly evolving nature makes it difficult to prevent, identify, track, trace and report. The trade in CSAM is designed in ways that makes it difficult to determine the jurisdiction of an investigation and obtain the required data/evidence to support prosecution. There may also be multiple jurisdictions involved if cryptocurrency was used. Depending upon the nature of the cryptocurrency utilized, the cryptocurrency could also make tracing the perpetrators less of a challenge.

Building trust

CSAM is used as currency by the perpetrators and obtaining this material ordinarily starts with online grooming. Vulnerable targets are identified by criminals through searches of the victims' social media or presence in online games. Once identified, victims are engaged via instant messaging applications like Telegram.

CSAM targets are "groomed" by bad actors in a variety of ways, including posing as their financial sponsor, talent scout, true love or best friend. Grooming takes place over time and similar to traditional "offline" human trafficking, it entails building trust through ongoing conversations and/or promising incentives to the victims. There can be financial incentives, the promise of fame by pretending to be the target's financial sponsor or talent scout, or perhaps the promise of true love.

The shame factor

As grooming progresses, and if it is increasingly successful, targets become victims as they are locked in and coerced into providing intimate details, photos, videos, as well as financial and personal information to the bad actors. As soon as these intimate details are collected by the criminals, either by internet fraud² or inadvertent or coerced disclosure, the bad actors adopt the "shame factor"³ and start their extortion by threatening to post the graphic content online for everyone to see.

Other than the aforementioned, some of the CSAM from the Nth Room case was provided by the minors' family members who voluntarily uploaded the photos and videos in order to gain trust and be invited to various rooms.⁴ This was part of the modus operandi of the Nth Room—a membership-based service to exchange sexual exploitation materials in different themed rooms. For example, the "Gotham Room" was the marketing room where members shared CSAM with each other, and the "Loli Room" (derived from the term Lolita complex) contained sexually objectifying videos of young girls. Providers of the CSAM content are referred to as "Doctors" and are paid for uploading content to the "Doctor's Room."⁵ Some play both roles (buyer and provider) in order to gain access to more prohibited materials.

Cruel statistics

Buyers of Nth Room content made bitcoin payments ranging from 250,000 South Korean won (\$217.32) up to 1,550,000 million South Korean won (\$1,347.39) equivalent to view.⁶ Sickeningly, since the Nth Room started in 2018, the CSAM content uploaded includes cruel self-harm content in addition to pornography.

To date, more than 3,700 clips of pornography have been discovered⁷ and more than 100 suspects have been arrested. There also appeared to be 260,000 users of 56 monitored chats on Telegram. The Nth Room is supported by a disturbing group of people who greet one another with “Let’s rape” in lieu of “Hello.”⁸

Know your customer

The existence of the Nth Room was fortunately exposed by two Korean female university students who in 2019 heard about the exploitation⁹ and began their investigation for an investigative journalism competition. The article, titled “Do you sell child porn?... Crime flourishing on Telegram,” gave insight into the sexually explicit chats the two engaged in while undercover that led to the eventual arrest of the mastermind behind the Nth Room. The South Korean man nicknamed “GodGod” was sentenced to 34 years in prison.¹⁰ Ironically, it was also revealed that GodGod requested know-your-customer documentation from prospective members to screen and verify their identity before they were allowed to participate in the exchange of CSAM.

Pedophilic disorder

The demand for CSAM leads to its supply and profitability. Anti-financial crime and law enforcement professionals regularly discuss child sexual abuse, human trafficking and modern slavery as crimes that must be prosecuted and punished. However, the eradication of CSAM at a global level requires education and awareness about diseases like pedophilic disorder and possible treatment options. Pedophilic disorder is characterized by recurrent, intense sexually arousing fantasies, urges or behaviors involving prepubescent or young adolescents (usually 13 years old or younger). It is diagnosed only when people are 16 years old or older, and 5 or more years older than the child who is the target of the fantasies or behaviors).

The treatments available to individuals with pedophilic disorder include psychotherapy and drugs, such as antiandrogens; however, these individuals may avoid seeking treatment as clinicians and therapists have legal requirements to report suspicion of child sexual or physical abuse to authorities. These requirements vary by country. In addition, the diagnostic age guidelines apply to Western cultures but not to the many cultures that accept sexual activity, marriage and childbearing at much younger ages.¹¹ For these reasons, numerous child exploitation cases are disregarded, unreported and untreated. Considering some financial institutions (FIs) have an international presence, their platforms could be utilized to bring global awareness and cultural influence in preventing child exploitation by recognizing and treating pedophilic disorder.

Educating and empowering children to recognize and report exploitation must be placed at the forefront of combating child exploitation

The importance of education

Educating and empowering children to recognize and report exploitation must be placed at the forefront of combating child exploitation. One of the great challenges is that in some cultures, obedience to parents or elders has a higher importance than children’s rights. Therefore, sexual exploitation of children may be regarded as “a family matter” as opposed to a legal matter. The vulnerability of children to sexual abuse may increase with stressful home environments, low self-esteem and unmonitored access to technology.¹²

FIs are not only in the position to detect and report potential child exploitation, they can also use their platform to initiate youth programs to promote mental health and technology risk awareness. FIs can form alliances and support local or international organizations involved with children’s rights and safety. The WeProtect Global Alliance is one of the organizations where institutions and countries can join to increase global efforts to combat online child sexual exploitation.¹³ Another organization is the Virtual Global Taskforce (VGT), an international law enforcement alliance to address child sexual exploitation online.¹⁴ The Interfaith Alliance brings religious leaders from across the world, law enforcement, regulators and the tech industry together to combat child exploitation and promote the dignity of children.¹⁵

Working with law enforcement

Traditional FIs as well as cryptocurrency exchanges can trace potential proceeds of CSAM and report or cooperate with law enforcement agencies. In the Nth Room case, a number of cryptocurrency exchanges provided valuable assistance to law enforcement.¹⁶

The suppliers of online child sexual exploitation materials rely heavily on the internet for every stage of the process, from grooming and producing sexual content, to receiving payments for the materials

The pattern of transactions for suppliers and consumers of CSAM are different and the institutions will have to create specific detection rules to identify both sides of the transactions. The transactions for consumers are in small amounts using services to obscure the destination of the funds. The suppliers may operate an account similar to a business account, however, the nature of the business and the source of funds may be unclear. At times, multiple personal accounts may be used to conduct activities on behalf of the supplier.

Based on an analysis from Canada's Financial Transactions and Reports Analysis Centre's on disclosures and suspicious transaction reports related to online child sexual exploitation, consumer transactions were mainly outgoing transfers, through money services businesses, to jurisdictions of concern for child sexual exploitation, including the Philippines, Thailand, Colombia, the U.S., Ghana, Ukraine, Dominican Republic, Romania, Jamaica and Russia.¹⁷

Indicators of suspicion

The suppliers of online child sexual exploitation materials rely heavily on the internet for every stage of the process, from grooming and producing sexual content, to receiving payments for the materials. The suspicious indicators related to possible perpetrators, when taken together and in context, may include a combination of online purchases, app purchases, online gaming and gambling, the use of online video and communication technologies, as well as the use of online file storage. These transactions can involve payment processors.¹⁸

Some suppliers may offer the sale of online child exploitation using cryptocurrency, which was the case for Welcome to Video, the largest child sexual exploitation market by volume of content at the time of writing.¹⁹ This website was funded by bitcoin and traceable by law enforcement. It is believed that the suppliers may turn to private cryptocurrencies to avoid traceability as these coins add a third-party processor that hides the transaction records. In the Nth Room case, the suppliers were accepting payments in bitcoin to allow access via Telegram.²⁰

In cases where privacy coins may be utilized to obfuscate the source and the purpose of the activity, the pattern and the amount of the transactions in conjunction with negative media on the user can serve as indicators. For example, while investigating Welcome to Video, certain transaction amounts (e.g., 0.04 bitcoin or \$39) appeared more often than others, which may be fixed charges for certain materials. The equivalent value of these specific amounts in privacy coins can provide insight to the purpose of the transaction.

Although the purchase of child abuse material can be completed through any cryptocurrency account type, it is more likely for these purchases to occur on accounts that are opened for the purpose of conducting these transactions and the chances of other transactions or trading activity are minimal. South Korea has been courageous to share the Nth Room case and its details with the world to offer a better understanding of online child exploitation and its possible detection and prevention methods. Other countries will need to follow this example and disclose the identity of the perpetrators for the safety of the public, especially children.

The role of social media

The global pandemic has increased the production of online child abuse material where the predators utilize applications that are "kid friendly" to meet and exploit children.²¹ The issue of child exploitation is not specific to one platform and extends across social media. There is a continued debate on how much responsibility social media companies must have in regards to regulating or policing what users post.²² Canada and other members of the Five Eyes intelligence alliance (the U.S., the United Kingdom, Australia and New Zealand) issued a statement that commits to pushing global tech companies to adopt a set of voluntary principles around the identification, disclosure and removal of online child sexual exploitation content. This is in addition to these countries' efforts in enhancing their ability to pursue and prosecute child exploitation offenders, as well as creating legislation to compel social media companies to improve the policing of child exploitation content.²³

The issue of child exploitation is not specific to one platform and extends across social media

The role of social media and the European Union

A new temporary legislation was also passed by the European Parliament in response to the aforesaid voluntary principles in which scanning technologies are allowed to detect online grooming against the backdrop of the European Union's (EU) ePrivacy Directive. It would be significant if the protection by the governments can be mandated by empowering officials with the ability to sanction or oblige noncompliant entities, in this instance, the electronic service providers.²⁴

According to the July 24 communication from the European Commission to the European Parliament,²⁵ "...Europol's ability to support the Member States is hampered by its inability to receive personal data directly from the private sector...." This would then confirm that the legislation currently available still limits the EU and other jurisdictions to anticipate voluntary disclosures only passively from electronic service providers. In the event of nondisclosure, the specific electronic service provider that operated and facilitated CSAM dissemination continued with their business unimpeded and unpunished. It is understood that data privacy is necessary in today's society. However, having to rely on voluntary disclosure



with respect to CSAM dissemination creates a huge vacuum that distastefully protects the perpetrators only. There must be a mechanism on a global scale to compel and encourage disclosure as well as penalty and recourse for nondisclosure to make this voluntary disclosure policy conducive and meaningful.

In conclusion

Human trafficking (more recently categorized as modern slavery) has been around for a long time and it grew significantly with the advent of the internet and modern communications.


Cybercrime in its various forms has evolved in more recent times as a profitable threat. When combined with the discussed twist of victims' self-publishing content in what Europol terms "self-exploitation" fueled by the COVID-19 crisis, cybercrime has taken on another form of sophistication as criminals seek every advantage to make illicit profit while minimizing the risks to themselves.

The Nth Room case and the referenced materials provide useful and real examples from an Asian and European perspective of recent criminal methodologies, which may amend or add to established indicators of suspicion and knowledge of how these cases work.

In researching and writing this article, the authors asked themselves, how can ACAMS members stop this exploitation?

Working collectively, ACAMS professionals can continue to make a positive difference in addressing these crimes by being alert to their existence, understanding how they work and ultimately sharing suspicions with law enforcement.

Peer input from members and readers is welcome. As the authors have examined the chain of victimization, they have identified potential solutions to be considered from the perspectives of phishing and grooming prevention, perpetrator identification, payment detection as well as services and operations.

FIs can participate in the prevention, detection and reporting of CSAM. FIs' platforms can also be utilized for bringing awareness on the topics of CSAM and methods of prevention. 

Shann Lu, LL.M, CAMS, AML & fraud financial investigation management, Bitfinex

Fara Fallah, CAMS, CGSS, CBP, CCI, compliance consultant, Bitfinex

Editing and additional content: Peter Warrack, CAMS, CBP, CCI, CFE, chief compliance officer, Bitfinex

¹ "Exploiting isolation: sexual predators increasingly targeting children during COVID pandemic," *Europol*, June 19, 2020, <https://www.europol.europa.eu/newsroom/news/exploiting-isolation-sexual-predators-increasingly-targeting-children-during-covid-pandemic>

² "Internet Fraud," *FBI*, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud>

³ Nicole de Souza, "The Nth Room case and modern slavery in the digital space," *The Interpreter*, April 20, 2020, <https://www.lowyinstitute.org/the-interpreter/nth-room-case-and-modern-slavery-digital-space>

⁴ Yoon So-Yeon, "The spark that ignited the 'Nth room' fire," *Korea JooAng Daily*, March 31, 2020, <https://koreaajoongdailyjoins.com/2020/03/31/features/The-spark-that-ignited-the-Nth-room-fire/3075527.html>

⁵ Ron Kim, "Victim Of Telegram Nth Room Case Speaks Up About The Horrors She Faced As A Middle School Student," *Koreaboo*, March 24, 2020, <https://www.koreaboo.com/news/victim-telegram-nth-room-case-speaks-horrors-faced-middle-school-student/>

⁶ Ibid.

⁷ Choe Sang-Hun, "South Korean Man Gets 34 Years for Running Sexual Exploitation Chat Room," *The New York Times*, April 8, 2021, <https://www.nytimes.com/2021/04/08/world/asia/korea-sex-crime-chat-rooms.html>

⁸ Haeryun Kang, "South Korea's 'nth rooms' are toxic mixture of tech, sex and crime," *Nikkei Asia*, April 10, 2020, <https://asia.nikkei.com/Opinion/South-Korea-s-nth-rooms-are-toxic-mixture-of-tech-sex-and-crime>

⁹ Yoon So-Yeon, "The spark that ignited the 'Nth room' fire," *Korea JoongAng Daily*, March 31, 2020, <https://koreaajoongdailyjoins.com/2020/03/31/features/The-spark-that-ignited-the-Nth-room-fire/3075527.html>

¹⁰ Choe Sang-Hun, "South Korean Man Gets 34 Years for Running Sexual Exploitation Chat Room," *The New York Times*, April 8, 2021, <https://www.nytimes.com/2021/04/08/world/asia/korea-sex-crime-chat-rooms.html>

¹¹ George R. Brown, MD, "Pedophilic Disorder," *Merck Manuals Professional Edition*, <https://www.merckmanuals.com/en-ca/professional/psychiatric-disorders/paraphilic-disorders/pedophilic-disorder>

¹² "11 Factors That Increase the Risk of Child Sexual Abuse," *Defend Innocence*, <https://defendinnocence.org/child-sexual-abuse-risk-reduction/proactive-parenting/reduce-risk/11-factors-that-increase-the-risk-of-child-sexual-abuse/>

¹³ *WeProtect Global Alliance*, <https://www.weprotect.org/>

¹⁴ *Virtual Global Taskforce*, <http://virtualglobaltaskforce.com/>

¹⁵ "Areas of Focus," *Interfaith Alliance for Safer Communities*, <https://iafsc.org/areas-of-focus/child-dignity-online>

¹⁶ Felipe Erazo, "Huobi Korea Delists XMR Amid Nth Room Sexual Exploitation Case Rumors," *Cointelegraph*, April 12, 2020, <https://cointelegraph.com/news/huobi-korea-delists-xmr-amid-nth-room-sexual-exploitation-case-rumors>

¹⁷ "Operational alert: Laundering of proceeds from online child sexual exploitation," *Financial Transactions and Reports Analysis Centre of Canada*, December 2020, <https://www.fintrac-canafe.gc.ca/intel/operation/exploitation-eng>

¹⁸ Ibid.

¹⁹ "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin," *U.S. Department of Justice*, October 16, 2019, <https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child>

²⁰ Scott Ikeda, "South Korea's New Crypto AML Law Bans Trading of 'Privacy Coins' (Monero, Zcash)," *CPO Magazine*, November 17, 2020, <https://www.cpomagazine.com/data-privacy/south-koreas-new-crypto-aml-law-bans-trading-of-privacy-coins-monero-zcash/amp/>

²¹ "Online Child Sexual Exploitation," *Government of Canada*, <https://www.canada.ca/en/public-safety-canada/campaigns/online-child-sexual-exploitation.html>

²² Aaron Barr, "Social Media Regulation: The Line Between Privacy and Protection," *Security Boulevard*, June 9, 2021, <https://securityboulevard.com/2021/06/social-media-regulation-the-line-between-privacy-and-protection/>

²³ Karen Pauls, "New rules on removal of illegal online content could help in battle against child pornography," *CBC*, January 4, 2021, <https://www.cbc.ca/news/canada/manitoba/canada-illegal-online-content-child-porn-1.5847695>

²⁴ "Five Country Statement to EU to prevent child abuse online," *Ministers for the Department of Home Affairs*, January 13, 2021, <https://minister.homeaffairs.gov.au/peterdutton/Pages/five-country-statement-EU-prevent-child-abuse-online.aspx>

²⁵ "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - EU strategy for a more effective fight against child sexual abuse," *European Commission*, July 24, 2020, https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf

How to incorporate money laundering risk into risk management:

Part one

Relavant provisions have regulated the incorporation of money laundering and terrorist financing risk (hereinafter referred to as money laundering risk) into the overall risk management of financial institutions (FIs). These provisions include the Financial Action Task Force’s “Risk-Based Approach Guidelines for the Banking Sector” issued in 2014, the Basel Committee’s “Sound management of risks related to money laundering and financing of terrorism” guidelines issued in 2017, the China Banking and Insurance Regulatory Commission’s “Administrative Measures for Combating Anti-Money Laundering and Terrorism Financing by Banking Financial Institutions” issued in 2019 and more.

The “Guidelines for the Management of Money Laundering and Terrorist Financing Risks of Corporate Financial Institutions” (Yin Fan Xi Fa [2018] No. 19) issued by People’s Bank of China give detailed instructions on deepening the practice of the risk-based approach for corporate FIs. These guidelines also implement the “Opinions of the General Office of the State Council on Improving the Regulatory System of Money Laundering, Financing of Terrorism and Tax Evasion,” strengthening the anti-money laundering/counter-terrorist financing (AML/CTF) work of corporate FIs as well as strengthening effective prevention of money laundering and related criminal activities. However, many institutions still have doubts on how to incorporate the money laundering risk into the overall risk management of FIs and may even take a detour in practice. Based on the practice of supervision and the actual situation of FIs, the author will provide guidance on the following three aspects in a series of articles: risk assessment and measurement of money laundering risk, formulating risk management strategies for money laundering and implementing duties for senior executives.

This first article will discuss risk assessment and measurement of money laundering risk. Although the aforementioned guidelines and regulations include money laundering risk in the overall risk management framework of FIs, they do not give methods to assess and measure risk or how to measure the loss brought to FIs by this risk.





Risk assessment and measurement of the money laundering risk

In most cases and events, money laundering risks themselves do not bring direct risks nor direct economic losses to FIs, sometimes they even generate income. Instead, indirect risks or losses are produced. As stated by the Basel Committee, “the inadequacy or absence of sound ML/TF [money laundering/terrorist financing] risk management exposes banks to serious risks, especially reputational, operational, compliance and concentration risks.”¹ It is worth noting that these risks are interrelated. However, any kind of penalty on FIs may bring huge risks at the same time (e.g., costs due to batch financing and loan termination, claims against banks, investigation costs, asset freezes and loan losses). Moreover, investing limited and valuable management and operational resources to solve the problems caused by money laundering risk also imposes costs. “Guidelines on Risk Management of Money Laundering and Terrorist Financing of Legal Person Financial Institutions” (Yin Fan Xi Fa [2018] No. 19) reads “any money laundering risk event or case may bring serious reputation risk and legal risk, and may lead to customer, business and property loss.”

In addition to the anti-money laundering (AML) fine brought by “strong supervision and strict accountability” when FIs fail to take appropriate risk management policies, procedures and control measures diligently, it will increase the direct or indirect cost caused by money laundering risk. If FIs can continue to implement effective risk-based AML/CTF policies and procedures, these costs and losses can be reduced or avoided. Therefore, FIs need to assess the money laundering risk, measure the direct or indirect losses caused by money laundering risk, and directly reflect on their money laundering risk status, so that the money laundering risk management strategy formulated can match the money laundering risk status and systemic importance level faced by the institutions. The specific historical simulation method and the scenario analysis method to measure the direct or indirect loss caused by money laundering risk is described below.

Measuring the loss caused by the compliance risk

The Ministry of Supervision supervises FIs to perform AML obligations on behalf of the interests of the public to reduce the harm of money laundering to society. When FIs fail to fulfill the AML obligations, the regulatory authorities (including other jurisdictions) will impose penalties on the FIs. Not only can regulatory authorities impose fines, they can also order FIs to suspend businesses for rectification, suspend or stop certain businesses, not approve new businesses and increase the proportion of various funds (deposit insurance funds, investor protection funds, insurance guarantee funds, etc.).

Assume that the loss due to compliance risk is expressed by T1, the penalty loss is expressed by t11 and the probability of occurrence is expressed by p11; FIs are ordered to suspend a business for rectification, and losses are expressed by t12, the probability of occurrence is expressed by p12; the loss of suspending or stopping a business is expressed by t13, the probability of occurrence is expressed by p13; the loss of a new business is expressed by t14, the probability of occurrence is expressed by p14; increase the proportion of various types of funds turned in and the loss is expressed by t15, the probability of occurrence is expressed by p15; then the formula is $T1 = t11 \times p11 + t12 \times p12 + t13 \times p13 + t14 \times p14 + t15 \times p15$. Each FI can confirm the value of t11 and p11 according to the AML supervision intensity, frequency and the actual penalty of its registered place, branch location and foreign branch country or region, especially the penalties imposed on the same kind of institution, combined with the self-assessment result of its own money laundering risk and the potential violation facts found; similarly, the values of t12, p12, t13, p13, t14, p14, t15 and p15 can be determined in combination with actual or historical data.

Measuring the loss caused by the reputational risk

It is very difficult to evaluate the loss caused by the reputational risk. When an FI is exposed to the scandal of money laundering cases or adverse media following major administrative AML penalties, it may lead to the loss of customers (new and old customers). While revenue is reduced, it may even result in a run on the bank. In addition, the banks will treat the business (corresponding business, cross-border remittance, etc.) brought by the FI with caution, which will increase the “friction coefficient” of business development, consume the limited and valuable management and operation resources of the FI, lead to potential losses and even terminate the cooperative relationship with the bank. Suppose that the loss caused by reputation risk is expressed by T2, the loss from customer reduction is expressed by t21 and the probability of occurrence is expressed by p21; the loss of business is expressed by t22 and the probability of occurrence is expressed by p22; then the formula would be $T2 = t21 \times p21 + t22 \times p22$. Each FI can design a questionnaire according to the actual situation of its current or potential customers, sample and evaluate the actions that customers will take when they know that an FI has been exposed to a money laundering scandal or adverse media following major administrative AML penalties, and then evaluate the resulting losses. This way, it can confirm the values of t21 and p21; business losses—t22 and p22 values—can be determined according to the cost of various documents and information as well as the reduction of work efficiency according to the various documents and information needed to handle various interbank businesses.

Operational risk and concentration risk could directly cause losses; however, operational risk and concentration risk can be "amplifiers" of compliance risk, reputation risk and legal risk

Measuring the loss caused by the operational risk and concentration risk


Operational risk and concentration risk could directly cause losses; however, operational risk and concentration risk can be "amplifiers" of compliance risk, reputation risk and legal risk. Operational risk and concentration risk in FIs will increase the probability of other risks, which is more likely to lead to compliance risk, reputation risk, legal risk and then loss. Specifically, when there are operational risks in FIs, it is easy to make the internal control system of AML invalid, or even produce "internal and external collusion," which makes the internal control system of AML useless.

For example, the teller of a bank handled the "fake cash" business at the customer's request, which eventually led to the occurrence of money laundering cases and led regulatory authorities to impose a fine of 5 million yuan (\$773,167.95) on the institution. When there is concentration risk in FIs, there may be five manifestations in the money laundering risk: first, the counterparties are concentrated in the countries and regions with a high risk of money laundering; second, customers are concentrated in countries and regions with a high risk of money laundering; third, the transaction volume is concentrated in the businesses or products that have a high risk of money laundering; fourth, the transaction volume is concentrated in the customers that are at high risk of money laundering; fifth, the legal tools or legal arrangements controlled by the same beneficial owner form the representation scale and capital advantage or they form a large number of related transactions.

In conclusion, assuming that the total loss of FIs caused by money laundering risk is expressed by T, then $T = T_1 + T_2 + T_3$. Within a certain period of time, these losses need to be made up by FIs using capital or even by using provisions in advance.

To evaluate and measure the loss caused by the money laundering risk, this article only considers the common elements in practice. These risk elements will interact, and the occurrence of one risk element will affect the occurrence probability of another risk element. In addition, the influence of the communication and coordination ability and the public opinion guidance of FIs is not considered, and the loss caused by other money laundering risk elements is also not considered.

The method of money laundering risk assessment and measurement in this article needs to be improved, and people in the industry can study and explore other more advanced methods.

Part two will discuss formulating risk management strategies for money laundering. 

Liu Lihong, operations office, People's Bank of China, China

¹ "Guidelines: Sound management of risks related to money laundering and financing of terrorism," *Basel Committee on Banking Supervision*, June 2017, <https://www.bis.org/bcbs/publ/d405.pdf>

Measuring the loss caused by the legal risk

The loss caused by the legal risk mainly refers to legal actions initiated by a specific group of customers or harmed customers after a money laundering case occurs in an FI as well as the loss imposed on the FI in order to avoid the claim or compensation process. For example, a bank suffered a legal action due to a money laundering case abroad and the bank paid hundreds of millions of dollars in attorney fees for it. Suppose that the loss caused by legal risk is expressed by T3, the customer compensation is expressed by t31 and the probability of occurrence is expressed by p31; the attorney fee is expressed by t32 and the probability of occurrence is expressed by p32; then the formula would be $T_3 = t_{31} \times p_{31} + t_{32} \times p_{32}$.

MUSINGS FROM AFTER QUARANTINE CHAPTER 3: JOB SEEKERS STRIKE BACK



Please look for the first and second chapters of “Musings From Quarantine” on [ACAMSToday.org](https://acamstoday.org) under our Career Guidance column.

I have been recruiting in the anti-money laundering (AML), compliance and regulatory space for 13 years and have experienced two recessions during that time. The most valuable lesson I have learned is that recessions are as predictable as any other cycle—from a hiring perspective, at

least. My first day on the job was July 15, 2008. I remember because two months to the day later, this large bank with which I was only becoming familiar went bankrupt. Depending on who you ask, September 15, 2008, is when the dominoes started to fall after the Lehman Brothers’ demise. You received whiplash attempting to keep up with all the banks and companies merging, filing for bankruptcy or crying to the government for help. At the beginning—and at the deepest parts of a recession—the first victims are jobs,



especially low-income ones. My phone started ringing off the hook at the end of 2008 and did not stop until the beginning of 2010. The calls started trickling in at a more rapid pace, and then suddenly there were stories about people getting laid off en masse. In 2009, American Express filled auditoriums of people and laid them off all at once. Practically speaking, it makes sense. How do you lay off 50,000 people one by one?

The effects of recessions are usually unexpected. This company goes bankrupt; then that one. Then you realize the economy is a house of cards waiting for just the lightest breeze to topple it. The go-to Band-Aid for most companies is to lay off employees and save cash through operational costs. Massive layoffs accelerate, cause greater pain and anxiety, and lead to government intervention. Government intervention leads to stimulus checks and cash infusions from all



directions. The irony is that companies never stop hiring even when they are firing half their workforce. During both the Great Recession and the pandemic recession, there were millions of jobs that were actively open and not filled. What happens is that buyers control the market during recessions. Companies can cherry-pick candidates, which makes sense. There is more supply than demand. Millions of people take themselves out of the job market because the job market is in hibernation. Stimulus checks (hopefully) get unemployed people through the recession, and employed people cling to their jobs like their lives depend on it. As a result, people stay in homeostasis for a certain period (usually, a year or two). Then, the light starts appearing at the end of this very long tunnel.

People are starting to become much more active, in all senses of the word, as they detach themselves slowly from the economic, public health and social shackles of the pandemic. I have (literally) moved more the first half of 2021 than all of 2020. And the job market is hotter than a Death Valley cactus in July. In the U.S., more than 3.29 million jobs were added between March 2021 and July 2021 and the unemployment rate dropped to 5.4%.¹ In addition, 7.6 million employees still need to be added to private company payrolls to get to the employment rate in February 2020.² They said the Great Recession was the worst economic crises since the Great Depression. The pandemic depression and recession made the Great Recession look like a walk in the park.

However, the bounce back is even more pronounced. In April 2021, there were 9.3 million open jobs waiting to be filled.³ In April 2020, there were close to 5 million open jobs.⁴ Compare that to the bounce back during the Great Recession: There were 3.5 million jobs going into January 2012. At the lowest point, in November 2009, there were 2.4 million open jobs according to data from the U.S. Bureau of Labor Statistics.⁵ What the U.S. is experiencing now (as of June 2021) reminds me of exactly what happened after the darkest times of the Great Recession. So job seekers—currently employed or in between jobs—can take advantage of the organic cycles of recessions.

While the Great Recession had the Dodd-Frank Act, the pandemic recession has vaccines. In 2010, Dodd-Frank created a slate of new positions out of thin air inside and outside of compliance and AML. In 2021, vaccinations against COVID-19 are allowing people to go outside and reopen the economy. In addition to the millions of new jobs that were created, companies are announcing that they plan to hire hundreds and thousands of employees now and in the future.⁶ The job market coming out of this recession, like those in the past, is a sellers' market. Candidates will have the upper hand as they receive and leverage multiple offers.

There are also other factors adding to the recruiting frenzy that is currently taking place, especially in the compliance, AML and regulatory space. The first factor is the fintech renaissance. Last year banking and financial services had to go digital. Most people were banking and investing from home. Alternative remittance, cryptocurrency wallets and exchanges, as well as robo-advisers increased staff across the board. AML and compliance teams certainly grew. The second factor is more of a nuance of the

pandemic recession. This recession was not the result of a fundamental flaw in the economy, which was the case in the Great Recession. Projects were put on hold because employees had to adjust to a new way of living and working quickly. Those projects are now back on the table and require additional staff immediately. The last factor is the government. The U.S. now has a Democratic federal administration, which usually equates to more regulation and enforcement. Add all these factors up and you get a recruiting boom. These upcoming 12-to-18 months will be interesting as there are, and will continue to be, too many open roles and not enough people to fill them. This is across all industries; AML and compliance are no different.

Words of wisdom

Many people thrived during the quarantine. They lost weight and hit peak fitness, discovered new hobbies, got better at their jobs, or a combination of all the above and more. Others did not fare as well. They lost their jobs, homes, health and family members as well as loved ones. The pandemic that will make 2020 live in infamy changed life for all so quickly. Now, people are starting to see the semblance of pre-pandemic times. Those small things in life we took for granted but we missed instantly: seeing our families for no reason, going to a fast-food joint and grabbing a beer at our local bar. Hopefully, we do not take them for granted again.

The job market is getting its groove back, and it is your turn to take advantage of it. How, as a job seeker, do you take advantage of a recession ending? Specifically, how do you take advantage of the pandemic recession ending?


1. **Start looking now:** The number of projects and full-time roles in AML and compliance will only increase. However, that does not mean you will get a job just because you want one. You have no idea how many people I work with that bang their heads against the wall because they are not getting the number of interviews and offers they were expecting. Then they lose steam and take themselves out of the market in

frustration. Those that stick it out and look for the right position end up having another problem: They end up having multiple offers and do not know which one to pick.

2. **Seek more skills and not just more compensation:** I have been championing this philosophy since I started writing for *ACAMS Today*. More skills equate to more compensation. Or, at least, more skills equate to more options. In addition to technology and artificial intelligence becoming a more significant part of AML and compliance programs in the legacy banking space, fintech and regtech companies are seeking technologically savvy compliance professionals. Use this time and opportunity to search for a job that will open more doors to learning new ways of executing as well as managing an efficient and streamlined compliance function.
3. **Do yourself a favor and do not expect all jobs to be 100% remote:** Do not say no to potential roles off the bat if 100% remote work is not on the table. Hybrid and remote work are now part of our lives but do not assume all roles have a 100% remote option. We will be going back to the office in some capacity. We transitioned to working remotely abruptly and under duress back in March 2020. We did not make the transition organically. Executives are going to want their employees back in the office.
4. **Work your network:** We all could network the conventional way during the Great Recession: lunches, conferences, coffees and cocktails. Before the end of social distancing restrictions, it was meetings on Zoom, Microsoft Teams and Google Hangouts. Guess what? There is no difference. Reach out to former colleagues and bosses, connect with new and potential contacts on LinkedIn and attend virtual conferences. Lastly, think about attending ACAMS conferences and events that your local chapter is hosting as they start returning in person.
5. **Your career path is not set in stone:** One of the best times to consider changing careers, industries and geographies is following a recession. Sellers' markets allow us to control not only our conventional job searches, but also our purpose and missions. What if compliance and AML has treated you well but your gut (maybe even your heart) is telling you that part of your life has run its course? In a hot job market, companies are getting desperate to find personnel. Take advantage of that desperation! Companies are open to creative ways to fill their headcount. With there being more open jobs than qualified candidates and job seekers, 2021 and 2022 will be excellent years to go outside your comfort zone.
6. **Use recruiting professionals (for free):** This is not a self-serving statement. Agency recruiters are free sources of information on the job market, your shared industry, trends in hiring, skillsets in demand, and, of course, jobs. Whether you are actively looking or passively keeping an eye open, leverage your trusted professional advisors. Consider agency recruiters part of your growing network in your work community.

By the end of 2021, hundreds of thousands of people will likely reenter the job market. A large segment of the working population who will be seeking employment are those who took themselves out of the workforce to take care of children who were being homeschooled, or because they were receiving state and federal funding that compensated them better than their jobs. Children will be returning to in-person teaching and federal and state funding will end. As a result, the economy will become red hot and the unemployment rate will drop to pre-pandemic levels. The irony is that many full-time permanent positions are on hold because of the labor shortage. Companies are engaging contractors and consultants to start projects in the meantime and waiting for the influx of new candidates. Thousands and thousands of jobs will be added in addition to the millions that are already open. It will remain a sellers' market.

Conclusion

This is the right time for job seekers. By implementing the recommendations of flexibility, learning and expanding your network and by taking control of your future in a market that caters to the job seeker, you will be able to leverage the best career or job for your needs. Who knows, you might end up with a career that pre-pandemic was not possible but has now turned into your dream job. 

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

Contributor and editorial input: Karla Monterrosa-Yancey, CAMS, editor-in-chief, ACAMS, FL, USA, editor@acams.org

- ¹ "Civilian unemployment rate," *U.S. Bureau of Labor Statistics*, August 6, 2021, <https://www.bls.gov/news.release/empsit.nr0.htm>
- ² Scott Horsley and Andrea Hsu, "Hiring Picked Up Last Month, But The Economy Still Needs More Workers," *NPR*, June 4, 2021, <https://www.npr.org/2021/06/04/1003035263/hiring-picked-up-last-month-a-relief-for-an-economy-desperate-for-workers>
- ³ Jeff Cox, "Job openings set record of 9.3 million as labor market booms," *CNBC*, June 8, 2021, <https://www.cnbc.com/2021/06/08/job-openings-set-new-record-of-9point3-million-amid-economic-reopening.html>
- ⁴ "Job openings, hires, and separations levels, seasonally adjusted" *U.S. Bureau of Labor Statistics*, <https://www.bls.gov/charts/job-openings-and-labor-turnover/opening-hire-seps-level.htm>
- ⁵ "Job Openings and Labor Turnover Survey News Release," *U.S. Bureau of Labor Statistics*, March 13, 2012, https://www.bls.gov/news.release/archives/jolts_03132012.htm
- ⁶ "Amazon to hire 100,000 more workers in its latest job spree this year," *CNBC*, September 14, 2020, <https://www.cnbc.com/2020/09/14/amazon-to-hire-100000-more-workers-in-its-latest-job-sprees-this-year.html>; Jessica DiNapoli, "PwC to Create 100,000 New Jobs to Help Clients Grappling with ESG Reporting," *Insurance Journal*, June 16, 2021, <https://www.insurancejournal.com/news/international/2021/06/16/618744.htm>

MAKING EVENT TRIGGER REVIEWS WORK



Event trigger reviews (ETRs) or event-driven reviews are part of the anti-financial crime (AFC) controls of ongoing monitoring or ongoing reviews. Unlike periodic reviews, which follow a cycle, ETRs are ad hoc. In addition, ETRs differ from anti-money laundering (AML) investigations as ETRs are usually undertaken by the business and not compliance.

This article will discuss how to make ETRs more effective toward managing a financial institution's (FI) client risk.

Regulatory expectations

The regulatory expectation is clear. During an ETR, the FI is required to update customer information and check if a client's risk profile needs to be reviewed. For example:

“After establishing a business relationship, FIs are required to maintain current and accurate knowledge of their customers through the performance of periodic reviews and/or reviews based on trigger events, and where appropriate enhance the frequency and intensity of customer engagement where the risks are assessed to be greater.”¹

ETRs supplement periodic reviews to ensure that client profiles are updated. However, as part of their risk-based approach, some FIs rely entirely on ETRs to update the client's customer due diligence (CDD) and risk profiles. However, ETRs do not appear to be effective. For example, in the statement of facts for ABN AMRO Bank's recent criminal investigation, Dutch prosecutors² noted that the following had not functioned properly in the bank:

- Within private banking ETRs were only carried out to a limited extent, meaning there was no ongoing monitoring of private banking business relationships.
- The bank's systems and processes that should have generated the information to trigger ETRs did not function properly as noted by the following examples:
 - Until September 2018, the bank's screening process for negative media coverage was not carried out automatically but manually. In addition, there was a backlog in processing screening hits and the ensuing reassessment of the impacted clients' profiles. In 2019, auditors found that the client filtering process was “marginally satisfactory and needed improvement.”
 - The transaction monitoring (TM) system missed several signals because of the risk classification used and how the system was set up. Moreover, there were backlogs in processing the generated TM alerts at least until 2019. Thus, the alerts that could lead to an ETR were not available on time.

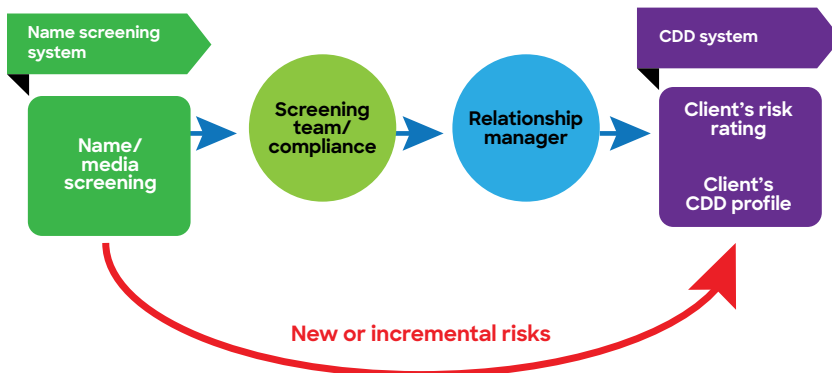
Assessment of new and incremental risk

After client onboarding, back-end name or media screenings routinely screen the FI's client database against vendor databases and internal blacklists for new or incremental risks. These risks include new politically exposed persons (PEPs), material adverse media or potential sanction nexuses against the client or its connected parties. The identification and escalation of these risks appear to be the standard ETRs for most organizations (see Figure 1).

However, the escalation protocol and the rubrics of the client risk assessment must be clearly defined. As new or incremental risks are identified, there must be a prompt tagging of the new risk in the FI's CDD system while the assessment is undertaken and exceptional approvals to retain the clients that are sought.

Aside from backlogs in reviewing screening matches (or hits), the real risk is that clients may not be tagged as higher risk while the business and compliance discuss new or incremental risks. For example, is the client a PEP? Is the adverse media material? Is the sanction nexus rather remote? Another risk is that the client has yet to be tagged as high risk because senior management approval is being sought to retain the client relationship. However, as long as the client is not tagged on the FI's CDD system, the client will not be subject to enhanced monitoring. As the risk indicators in the FI's CDD system feed into the TM systems for monitoring according to risk-defined thresholds, the rule should be to tag first, then decide.

Figure 1: Assessment of new and incremental risks



The TM loop back

During TM and in response to a request for information (RFI) from the TM team, the client may give information to explain away an alerted transaction. For example, the client's counterparty may be their new employer or supplier; on the other hand, they may be the client's other private investment company or relative. The client may also disclose a new source of wealth or funds when explaining the purpose of the alerted transaction. This new information was not found in the client's CDD profile with the FI, hence the RFI. But how often does this information just sit in the audit log of the closed alerts in the FI's TM case management system?

An effective loop-back mechanism triggers an ETR from TM to the relationship manager. Upon receipt, the relationship manager reviews and includes the additional information in the client's CDD profile. As part of the ETR, the relationship manager should also assess if the client's risk needs to be reprofiled and whether the client's stated intended purpose of the account and anticipated account activity in the CDD profile need to be revised. The revised

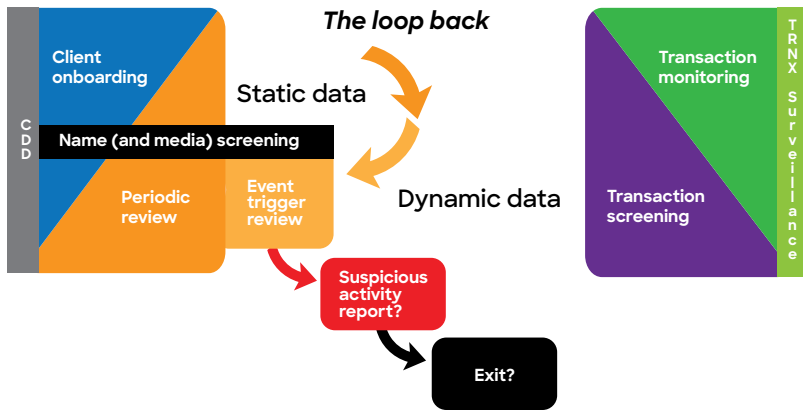
CDD profile on the FI's CDD system enables the TM team to assess the risk relevance of the next TM alert against the same client quickly (see Figure 2).

As new information may also be disclosed by the client in response to an RFI to resolve a potential transaction screening match (or hit), the loop-back mechanism should also be deployed to relay information from the screening team to the relationship manager for an ETR. As a transaction screening match usually relates to a potential sanctions nexus of the client or their counterparty, the client's response to the RFI should be included in the client's CDD profile. The new information becomes part of the sanctions due diligence of the client, especially when the new information discounts the potential match against the client or counterparty as a false match.

Trigger rereview of the source of wealth and source of funds

For private banking clients and higher-tier retail clients, the source of wealth (SOW) and the source of initial funds are required to be corroborated or verified during client onboarding. This requirement is for the bank to assess the legitimacy of the client's total wealth (namely net worth) and source of funds (SOF). After onboarding and completing periodic reviews, relationship managers routinely ask for changes, if any, in a client's stated SOW or SOF. But does the bank provide for an ETR when the incoming transaction size (either singly or as an aggregate) exceeds the client's stated net worth? Or is there an ETR whenever the assets under management (AUM) exceed the client's net worth? The transaction size and increased AUM suggest that the bank may not know the client's total wealth or SOF.

Figure 2: The loop-back mechanism



A bank should develop a quarterly or semiannual dashboard where significant incoming remittances and substantial increases in the client’s AUM are automatically flagged out to the relationship managers. The dashboard should also flag out when the client becomes a large client or a significant relationship (i.e., where the AUM equals or exceeds a given threshold.). The dashboard is an additional control to TM and its suite of detection scenarios.

As part of the ETR, the relationship manager should review if their client’s stated net worth has been exceeded and inquire with the client about their new SOW and SOF. Furthermore, when the client becomes a “large client” or a “significant” relationship, the ETR is essentially a reexamination of the client’s SOW and SOF, as well as an assessment of the new or incremental client risk, if any. The new SOW and SOF should be documented and corroborated. Where the client’s risk has increased, the AFC policy should also provide for exceptional approval to retain the client relationship. An illustration of the dashboard can be seen in Figure 3 below.

Figure 3: Dashboard for a net worth review trigger

Client name				
Account number				
Net worth stated as of DD/MM/YYYY		\$X		
	Q1 YYYY	Q2 YYYY	Q3 YYYY	Q4 YYYY
Transaction size (\$,000)	500	50	2,000	
AUM (% increase)	3	No change	5	
AUM (Large client)				Yes
Note: The AFC policy defines significant transaction size and substantial increase in AUM, both in relation to the stated net worth. The policy also defines a large client by their AUM with the organization.				

Integrating best practices for effective ETRs

- The FI’s AFC policy should clarify what an ETR is, the trigger events or drivers when a client’s CDD profile is to be reviewed and when the client’s risk is to be reassessed.
- Clarify the roles and responsibilities for an ETR, including the escalation protocol.
- Design system process flows for the automatic relay of the triggers (and information) to the relationship manager to undertake an ETR.
- Ensure that there are sufficient resources for the timely review and disposition of alerts and matches, and consequently, timely ETRs.
- Track ETRs to completion. This includes checking that the client’s risk rating has been revised and that their CDD profile has been updated on the FI’s CDD system, where applicable.

Conclusion

Effective ETRs are an integral component of an effective risk-based AFC program. Therefore, FIs should design and ensure compliance with the ETR process. Having updated client CDD and risk profiles following ETRs will result in better AFC risk management.

Rosalind Lazar, CAMS, regional AML director-APAC, ACAMS, rlazar@acams.org

¹ “Guidance For Effective AML/CFT Transaction Monitoring Controls,” Monetary Authority of Singapore, September 2018, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidance-for-Effective-AML-CFT-Transaction-Monitoring-Controls.pdf

² “Statement of Facts and Conclusions of the Netherlands Public Prosecution Service,” National Office for Serious Fraud, Environmental Crime and Asset Confiscation (Functioneel Parket) and National Office (Landelijk Parket), https://assets.ctfassets.net/1u811bvgvthc/4eUXF7eCnLthKp95RNnMnz/645730a7cd044da33ef4ad1545470f12/Statement_of_Facts_-_ABN_AMRO_Guardian.pdf



Greater Phoenix Chapter: Pivot, evolve and adapt!

The ACAMS Greater Phoenix Chapter hosted a virtual webinar in June titled, “Terrorist Financing in the Crypto Age: Regulatory and Law Enforcement Framework.” The event had over 500 registered participants and proved to be a true crowd pleaser. Chris Janczewski, special agent for the IRS Cyber Crimes Unit, kicked off the show with three true crime examples of how terrorist organizations “pivot, evolve, and adapt” their financing methods, specifically with cryptocurrency. Agent Janczewski demonstrated how U.S. law enforcement successfully seized websites and currency assets of organizations tied to Hamas, al-Qaida and the Islamic State (IS).

One organization used their website as a bitcoin fundraising campaign seeking donations for the “Palestinian resistance,” while another used its Telegram channel to request donations to fund attacks and support “the mujahidin in Syria.” An IS facilitator created a website claiming to have inventory of N95 and other personal protective equipment for sale in a time of crisis. Victims paid for nonexistent inventory with credit cards and these cards were compromised. Criminal proceeds totaling \$100,000 were then laundered through bitcoin, and the facilitator was caught! Thankfully for the U.S. government, the crypto seized through these operations has appreciated over time—a bit of a cherry on top of that proverbial sundae.

Next up was Ari Redbord from TRM Labs. Redbord introduced TRM’s mission to “prevent cryptocurrency fraud and financial crime to build a safer financial system for billions of people.” He stressed his perspective that crypto is poised for explosive growth and bad actors use new techniques to evade detection—techniques such as chain-hopping, privacy technology and programmatic money laundering. The focus of his presentation was the current regulatory landscape as it relates to crypto: a strong focus on illicit use of the currency with minimal focus on its lawful use, even though less than 2% of on-chain transactions on Bitcoin are linked to illicit entities.

Redbord noted that the U.S. Treasury Department, including the Financial Crimes Enforcement Network, remains focused on the illicit use of crypto as evidenced by the current regulatory requirements placed on virtual asset service providers—licensure, know your customer and enhanced due diligence, transaction monitoring and Travel Rule compliance. He pointed out how similar these requirements are to those of financial institutions (FIs), which presents challenges! FIs act as intermediaries and are positioned to collect financial intelligence and push it up an organizational structure to law

enforcement. However, cryptocurrency is decentralized. Its structure does not follow the typical organization, and criminals challenge the intelligence gathering with tactics of chain-hopping and privacy technology. How the regulatory industry pivots, evolves and adapts is yet to be seen.

The highlight of the show was the audience, hands down! The Q&A session lasted nearly an hour and there were still questions in the pipeline. The ensuing discussion took the chapter down a journey of topics such as the use of antiquities to finance terror, domestic terrorism case nuances, issues in getting ahead of newer cryptocurrencies with faster transaction times, and a virtual brainstorming session on how to mitigate risks across the industry. Most impactful to this author, Agent Janczewski reflected on the distinction between completely dismantling a terrorist organization and a seemingly less impactful feat of disrupting their financing or operations. At the end of the day, you take the win! 

Caryn Langolf, CRCM, CAMS,
communications co-director,
ACAMS Greater Phoenix Chapter,
carynlangolf@gmail.com

ACAMS Certifications

Enhance your workforce's knowledge, skills and expertise in financial crime prevention with an ACAMS Certification.

www.acams.org



The Gold Standard



Winnie Yuen:

Communication for effective collaboration

ACAMS Today chatted with Winnie Yuen, global marketing operations manager, about her marketing experience throughout the years and the keys to a successful marketing campaign. Yuen has worked in marketing communications for over 10 years. Before joining ACAMS, she gained and developed her marketing skills while working in the gaming and lifestyle industries. This month, Yuen is celebrating her fifth anniversary working for ACAMS. She was the first ACAMS marketing colleague hired in the Asia-Pacific (APAC) region, so she witnessed the ACAMS Hong Kong office become larger and larger with more and more energetic colleagues joining the office.

In the past five years, Yuen has overseen all marketing promotions in the APAC region from product launches to live conferences and from promotional emails to event giveaways. In 2019, she was honored with a TEACH award from Adtalem Global Education in recognition of her passion for delivering exceptional outcomes in service of ACAMS members and business partners. Recently, Yuen was promoted to global marketing operations manager where she acts as a bridge to connect and communicate with different divisions among the marketing team and she also works on cross-department projects.

ACAMS Today: Congratulations on five years with ACAMS! How did your marketing experience in the gaming and lifestyle industries translate to your marketing work at ACAMS?

WY: Thank you very much! I can't believe it's already been five years. The gaming, lifestyle and financial compliance industries look so different, but the basic marketing principles do not change. The experience that I gained from previous companies gives me more confidence on handling marketing challenges. There is a funny story about the first time I met Fernando Beozzo Salomao, ACAMS' global director of marketing, in person at the U.S. office. As we talked, we discovered that he and a former boss of mine knew each other because they worked for the same company and in the same division. What a small world!

AT: How has the APAC marketing department grown since you were the first and only colleague?

WY: When I joined ACAMS in 2016, I was the only marketing person working in APAC and doing all the marketing promotion for the APAC region. At that time, we had 10 live seminars and one live international conference happening all during one year, the Certified Anti-Money Laundering Specialist (CAMS) certification was being offered in APAC in four languages and there were other marketing projects in the works—you can imagine how much work it was for a one-man band. Fortunately, my hard work (and heavy workload) was recognized by management, so we started to grow our APAC marketing department to a four-person team in 2018. Now we have three Hong Kong-based marketing colleagues and one Beijing-based colleague. We all have different backgrounds and experiences, and I think it's a very good team mix.

AT: What are the keys to a successful marketing campaign?

WY: For me, the core of marketing is to connect consumers and the product/service. To have a successful marketing campaign, it's always important to know what our potential consumers need and what are their pain points. ACAMS is not a retail company, so we rely a lot on data analysis, survey feedback and communication with sales representatives because they are client facing. We also need to always be apprised about the industry/market news and movement.

AT: As global marketing operations manager, what advice do you have for collaborating across departments and across regions?

WY: Communication! Without communication, nothing will happen. This applies to all collaborations everywhere, but especially ACAMS because it is a big and global team. Everyone has their own strengths, experiences and standpoints; therefore, communication is essential to achieve common goals.

AT: What has been your most impressive ACAMS marketing project thus far?

WY: My first international conference and the launch of ACAMS' WeChat and LINE social media channels are two projects I consider to be very impressive. In 2017, I was the only marketing person working in the APAC region so there were tons of tasks to do before the conference. In addition, WeChat and LINE are social media channels that are highly used among Chinese-speaking users. That was my first time handling the launching of applications and launch planning, so there was a lot to learn about the process.

AT: What do you like to do in your spare time?

WY: I enjoy hiking, running and watching TV in my leisure time. But recently, I started learning about household repairs and the Thai language. I am still exploring new hobbies to try out—no exact criteria, as long as it's interesting and useful! 

Interviewed by: Stephanie Trejos, CAMS, editor, ACAMS, FL, USA, strejos@acams.org





ADVANCED CERTIFICATION GRADUATES

Graduates countries/regions are sorted alphabetically

Armenia

Emil Abrahamyan, CAMS-RM

Bahamas

Sinead Bethel, CAMS-RM

Cayman Islands

Christopher Green, CAMS-RM

Germany

Manuela Drachenberg, CAMS-RM

Hong Kong

Kit Wah Flora Liu, CAMS-RM

Siu Long Wong, CAMS-RM

Japan

Yasutomo Haruki, CAMS-RM

Latvia

Khaled Almustafa, CAMS-RM

Kalvis Bambals, CAMS-RM

Lebanon

Katia Marrouche, CAMS-RM

Macao

Ching Chi Percy Wong, CAMS-RM

Netherlands

Henri Korkalainen, CAMS-RM

Luciano Riccioli, CAMS-RM

Marcin Wasilewski, CAMS-RM

Norway

Adis Crnalic, CAMS-RM

Qatar

Faheem Razzaq, CAMS-RM

Saudia Arabia

Malcolm Sandesh Lewis, CAMS-RM

South Korea

Yoon Sang Seong, CAMS-RM

United Arab Emirates

Kartik Sharma, CAMS-RM

United Kingdom

Yoe Strous, CAMS-RM

United States

Mark Creizman, CAMS-RM

Christopher A. Freiermuth, CAMS-RM

Carlos Ludert, CAMS-RM

Christine Marie Mayer, CAMS-RM

Xiao Chin Mu, CAMS-RM

Brian Pfeiffer, CAMS-RM

Ronnie Augusto Salvador, CAMS-RM

Umamani Selvam Sukumar, CAMS-RM

PREMIUM WEBINAR SUBSCRIPTION

Your all-access pass to ACAMS Webinars



The **NEW** ACAMS Premium Webinar Subscription is an annual pass that offers unlimited access to the comprehensive ACAMS library of live and on-demand webinars.



9+ **NEW live webinars released**
each month on average



40+ **AFC topics covered**
each year



800+ **Hours of AFC training**
in the ACAMS library

Learn more and subscribe at

acams.org/en/premium-webinar-subscription

ACAMS Webinars are included with this subscription as well as available to Enterprise Members





CAMS GRADUATES: MAY-JULY

Graduates countries/regions are sorted alphabetically

Afghanistan

Atal Bahand
Izatullah Hafizi
Aimal Mangal

Armenia

Gevorg Khachatryan

Aruba

Kelvin Osmond Halley
André Carmelo Kelly
Sandy Odor
Albertico Gregorio Willems

Australia

Kwame Kyei A. Agyapong
Yuko Asakawa
Cihan Bahcesarar
Andrew Barnes
Christine Chandran
Yao Chen
Zhoufu Chi
Xue Ding
Shon Edward Fernandes
Cameron Gale
Salini Ganesan
Kevin Horan
Xiaonong Hu
Xingying Jiang
Mingying Jiao
Yang Ann Joo
Crisberne Agnello Joseph
Anusha Kathula
Ryan John Lawson
Shana Lay
Soo Min Lee
Lingxiao Li
Mengyu Li

Yilin Li
Cuixia Lu
Jodie Mahoney
Athithya Mayuran
Connor Oliver Murphy
Gregory T. T. Nasu
Jonathan Nathar
Venkatesh Nathilvar
Shabnam R. Koshkaki
Luke Matthew Raven
Emma Sacre
Vineet Satish Shetye
Barun Lal Shrestha
Harry Solanakis
Chi-Ping Sun
Kimberley Tarling
Arunthethy Thevaraja
Yudhistira Tiono
Qian Wang
Charlotte Peiwen White
Anthony Michael Youssef
Jiahua Yu
Bingxin Zhang

Austria

Amaury Crucy

Azerbaijan

Tural Imamaliyev

Bahamas

Crystal D. Bleasdel
Terrel Lawrence Butler
Makeba Darville Sands
Tyra K. Duncombe
Hubert Edwards
Anastacia Philippa Hepburn
Patrice Lamm

Kristin Leah Sands
Nekeisha T. Smith

Bahrain

Stuti Agarwal
Alla Alnahisi
Ali Alsawad
Rahul Appukkuttan Mukundan
Bowen Cai
Waqas Iftikhar
Feroze Isaac
Jiss Maria Jose
Sujith Surendra Nath
Muhammad Tariq
Ravi Kumar Uppu

Bangladesh

Shafayet Hussain Ahmed
Tahmina Akhter
Kazi Wares Ul Ambia
Kazi Hossain Ansary
MST Zannat Ara
Mohammad N. Chowdhury
Anup Das
Rajib Dey
Bishwarup Dhar
Nasimul Gani
Ranjit Gogoi
Md Monir Hossain
Md. Zakir Hossain
Md. Saiful Islam
Madhab Chandra Karmaker
Mohammad Golam Kibria
Shah Selim Hamid Ovi
Mohammad Saiful Islam
Md Nazmus Sakib
Md Salauddin
Aloka Sarah

Shatabdee Sen Sarma
Kazi Mazbah Uddin
Syed Mohammad Walid

Barbados

Dennice L. Bend
Tracia N. Forde
Kerryanne Gilkes
Anne-Marie Goddard
Rosson Howard
Shauna Kissoon
Kisha Simpson
Rasheda Melissa S. Walker

Belgium

Eduard Hovsepyan
Roger Kaiser
Anne-Dorine Ligthart
Thomas Mareel

Belize

Salvador M. Awe
Lissa A. Lord

Bermuda

Claire Loxley
Pui Shan Ma

Botswana

Malebogo Hirschfeld
Masego Matjola
Gorata Moipolai

Brazil

Renato Conde Canado
Rafael Batista Ocanhas
Hyde de Melo Silva
Paula Vergamini

Brunei

Mary Chiew Horng Ong

Bulgaria

Georgi Denkov
Aleksandar Tsvetkov
Pavel Zhelyazkov

Canada

Robert Adah
Opeoluwa O. Adenaike
Emmanuella Okoi Adole
Yara Ahmed
Akinyinka Akinoso
Shalina Angelo
John Athanasiades
Alex Chiedu Azubuike
Shitang Bakifon
Yvita Shane Laurent Baldoz
Azadeh Bell-Irving
Lynda Boisvert
Rebecca Marie Bukovcan
Luiza Carvalho
Colin Chin
Juan F. Contreras
Darryl Andrew Cox
Katarzyna Czekanska
Dennis Dai
Vishal De Silva
Annie Desautels
Rohit Dhurnal
Susan L. Dicks
Nicole Danielle Ferenc
Yasmine Garreau
Ami Ghadawala
Kashif Ghani
Jonathan Mark Giffin
Wojciech Gorski

Lancelot Graham
 Keisha Grosvenor
 Derek Hall
 Mitchell Hamlyn
 Margaret Oluwasayo Hamzat
 Dan Heinemann
 Chuan Yu Hung
 Manisha Jammihal
 Xiaoqi Jin
 Muhammad Nour Karmeh
 Seo Hee Kim
 Roma Koopla
 Darshan Kumar
 Regis Kumar
 Nibedita Kundu
 Ashwathi Lakshminarayanan
 Sin Ying Michele Lam
 Brenda Lampman
 Catherine Leger
 Janet Li
 Wanwan Li
 Marie Kimberly Lim
 Chun Wa Barry Lo
 Shane Luchun
 Josna Raju Manjrekar
 Hayatte Mechkour
 Mohsin S. Mukaddam
 Aarti Naidu
 Karin Lourdina Nanayakkara
 Khurram Nawaz
 Morounfoluwa Oduwole
 Ademola Ogungbemile
 Florence Ogunsanwo
 Karen Okura
 Oluwasegun Oladiran
 Oluwabukunola O. Omolaja
 Solomon O. Oyeniran
 Catherine Paquin-Veillette
 Verushka Patana
 Shailee Patel
 Nataliya Pejko
 Eldho P. Peter
 Mark Ross
 Neil Scott
 Amala Selvaraj
 Ndeye Arame Seye
 Kalpit Jagadishbhai Shah
 Shabbir M. Shabbir Shah
 Shivi Sharma
 Kirill Smirnov
 Crystal Stuart
 Alex-Anne St-Vincent
 Arpan Sur Chowdhury
 Brian Swallow
 Mashiyat Tabassum
 Anne Okimasi Takim-Ndifon
 Amélie Théberge
 Mac Thiele
 Jade Tordecilla
 Pui Ki Tsui
 Shane Viraght

Ana Vozian
 Junlin Wu
 Mark Wynter
 Jingwei You
 Samir Zariwala
 Ping Zhang
 Ge (Gary) Zhu

Cayman Islands

Edgar Ogville Bennett
 Deepal Bhandarkar
 Ashley Borde
 Kayla Bush
 Elizabeth Byrne
 Melissa Nastasia Durrant
 Hilda Farinas
 Kimberley R. W. Griffith
 Cassie Camille Knowles
 Nykemah Kuylen-Perera
 Nancy Manyange
 Robyn Elizabeth McCoy
 Christine C. Olukoya
 Lashonda Madiera P. Powell
 Sarai Soto
 Leonie Taber
 Sharon Taiy
 S. van Batenburg-Stafford

Chile

Valerie Nicole Mori Fernández

China

Yichao An
 Zejin Ban
 Jian Bao
 Haoyu Bi
 Shushu Bie
 Xianqun Bing
 Junrong Cai
 Lingchun Cai
 Ming Cai
 Wentao Cai
 Yiping Cai
 Weihang Cao
 Xiaodong Cao
 Zhiyu Cao
 Xuenan Chai
 Yubin Chai
 Yi Chan
 Xiaoxuan Che
 Dan Chen
 Danni Chen
 Fang Chen
 Fei Chen
 Guojun Chen
 Jiadao Chen
 Jian Chen
 Jing Chen
 Jing Chen
 Kaiyi Chen

Lei Chen
 Li Chen
 Liqin Chen
 Man Chen
 Meng Chen
 Peilan Chen
 Qingyang Chen
 Wenlin Chen
 Xiaoman Chen
 Xiaoxia Chen
 Xiaoyuan Chen
 Xinan Chen
 Xu Chen
 Yanan Chen
 Yang Chen
 Yangting Chen
 Yanjun Chen
 Yi Chen
 Yifei Chen
 Yuan Chen
 Yunyu Chen
 Yunyun Chen
 Ze Chen
 Zhaojing Chen
 Zhaorong Chen
 Zhihui Chen
 Ziqian Chen
 Fang Cheng
 Haiying Cheng
 Jin Cheng
 Kai Cheng
 Kailin Cheng
 Lili Cheng
 Shuxian Cheng
 Xinyue Cheng
 Yi Cheng
 Fangfang Chu
 Jishen Chu
 Ning Chu
 Wenyuan Cui
 Yingjie Cui
 Bifeng Dai
 Minglu Dai
 Wenqian Dai
 Xiaofeng Dai
 Xiaoling Dai
 Yinfang Dai
 Yue Dai Dai
 Mengzhe Deng
 Xinhui Deng
 Yating Deng
 Yunhong Deng
 Hao Ding
 Jian Ding
 Wen Jing Ding
 Xueliang Ding
 Ya Ding
 Yongxin Ding
 Jie Dong
 JingYi Dong
 Qinyuan Dong

Rui Dong
 Xin Dong
 Zihe Dong
 Chunyu Du
 Jiakuan Du
 Tianhao Du
 Tingting Du
 Wan Du
 Xian Du
 Xiaowei Du
 Yingying Du
 Jicheng Duan
 Yunliu Duan
 Beibin Fan
 Guoju Fan
 Juan Fan
 Meng Fan
 Xin Fan
 Yangyang Fan
 Hui Fang
 Yi Fang
 Chunpeng Feng
 Fan Feng
 Haitang Feng
 Jianao Feng
 Kalin Feng
 Xuejing Feng
 Yuan Feng
 Yuling Feng
 Jinbo Fu
 Jingou Fu
 Weinan Fu
 Bowen Gao
 Guangjian Gao
 Hairui Gao
 Jie Gao
 Jingwen Gao
 Lan Gao
 Ling Gao
 Shenghan Gao
 Tong Gao
 Wei Gao
 Xueyan Gao
 Yongfei Gao
 Zhoulu Ge
 Ping Geng
 Zhigang Geng
 Zihao Gong
 Liming Gu
 Xiaowei Gu
 Yajun Gu
 YiJing Gu
 Yu Guan
 Yue Guan
 Dandan Guo
 Hao Guo
 Jingyu Guo
 Lei Guo
 Ling Guo
 Mingyu Guo
 Shihua Guo

Xiujing Guo
 Yuli Guo
 Yuzhen Guo
 Jinru Han
 Lijun Han
 Miao Han
 Tong Han
 Xiaomei Han
 Xiwei Han
 Yutong Han
 Pengyu Hang
 Guoshu Hao
 Jingying Hao
 Liu Hao
 Chunxiao He
 Li He
 Lijuan He
 Qian He
 Xuejiao He
 Yixiong He
 Zhidong He
 Shanshan Hong
 Yan Hong
 Kaixuan Hou
 Zilong Hou
 Daohai Hu
 Guobin Hu
 Juan Hu
 Kuli Hu
 Tenggui Hu
 Tingyu Hu
 Xiaoyan Hu
 Zhongzhou Hu
 Fan Huang
 Heng Huang
 Hongmiao Huang
 Huang Huang
 Jiheng Huang
 Jing Huang
 Jinxu Huang
 Kaiyu Huang
 Ling Huang
 Minghui Huang
 Rui Huang
 Sheng'An Huang
 Tongxin Huang
 Weijie Huang
 Weizhong Huang
 Xiaohong Huang
 Xiaojuan Huang
 Xiaoping Huang
 Xiaoyuan Huang
 Xin Huang
 Yanghua Huang
 Yingxue Huang
 Zhenzhen Huang
 Tongtong Huo
 Xiaoli Ji
 Yue Ji
 Funing Jia
 Liangqin Jia

[GRADUATES]

Qifan Jia
Xiaoni Jia
Yinan Jia
Peng Jian
Yi Min Jian
Aijun Jiang
Bing Jiang
Bo Jiang
Fang Jiang
Kangding Jiang
Kun Jiang
Nan Jiang
Qun Jiang
Siyi Jiang
Wei Jiang
Yun Jiang
Xuejing Jiao
Yuehong Jiao
Rongzhou Jin
Shaoxiao Jin
Tian Jin
Dan Jing
Jiemin Jing
Bo Ju
Wenhua Kang
Baoqi Kuang
Jiangnan Lai
Xiuli Lai
ZhenAn Lai
Chubin Lan
Li Lan
Xiaolin Lan
Shuhua Lao
Aijie Li
Bailou Li
Bin Li
Bo Li
Chao Li
Chen Li
Chenyu Li
Congrong Li
Fang Li
Guangzhong Li
Guowei Li
Haocheng Li
Hong Li
Hui Li
Huimin Li
Jiahui Li
Jian Li
Jie Li
Jieqiong Li
Jing Li
Kan Li
Li Li
Lin Li
Lu Li
Lu Li
Meiyi Li
Menglin Li
Minli Li

Qian Li
Qing Li
Qinghua Li
Qiuyan Li
Ran Li
Ruiping Li
Sha Li
Shan Li
Shu Li
Sizhen Li
Subei Li
Suyang Li
Tian Li
Tingting Li
Weina Li
Weize Li
Xia Li
Xiafen Li
Xingpu Li
Xiyun Li
Xue Li
Xueyi Li
Yan Li
Yang Li
Yanrong Li
Yanyun Li
Yaoren Li
Youyuan Li
Yuan Li
Yuanbin Li
Yun Li
Zhenyan Li
Zhenzhu Li
Zhuoqian Li
Furong Liang
Jianbin Liang
Qianyi Liang
Zhouyu Liao
Chuancheng Lin
Fei Lin
Honghuan Lin
Jie Lin
Jing Lin
Miao Lin
Qi Lin
Renyi Lin
Xian Lin
Xiaofeng Lin
Yishu Lin
Yuejian Lin
Zhuoxi Lin
Yan Ling
Aiping Liu
Chuanqi Liu
Cong Liu
Dandan Liu
Gexu Liu
Haiwei Liu
Jian Liu
Jie Liu
Jie Liu

Jing Liu
Jingya Liu
Jun Liu
Jun Liu
Junhui Liu
Junyan Liu
Liquan Liu
Mengxi Liu
Naiwen Liu
Ni Liu
Qian Liu
Qiang Liu
Shang Liu
Tingting Liu
Weixu Liu
Xiangchen Liu
Xiaomeng Liu
Xuhong Liu
Xun Liu
Xuyang Liu
Yating Liu
Yexuan Liu
Yijie Liu
Ying Liu
Ying Liu
Yushan Liu
Zhuoqun Liu
Xiaoyu Lou
Jingli Lu
Xiaoyan Lu
Xiuting Lu
Ye Lu
Yinian Lu
Bin Luan
Luan Luan
Hao Luo
Kaifang Luo
Shihui Luo
Wei Luo
Yang Luo
Jiabin Lv
Jianxun Lv
Jing Lv
Pengfei Lv
Yang Lyu
Chunmin Ma
Fengming Ma
Jianlin Ma
Junhui Ma
Li Ma
Ruilin Ma
Xiao Ma
Xiaojuan Ma
Xiaoming Ma
Xiaoyang Ma
Xingwu Ma
Yuan Ma
Yunheng Ma
Jiayin Mao
Yujia Mao
Zhimeng Mao

Rui Mei
Juan Meng
Lijun Meng
Lin Meng
YanJun Meng
Ying Miao
Chuanqi Mo
Kaina Niu
Wenchi Ou
Jing Pan
Tianyu Pan
Yiting Pan
Cuiping Peng
Huize Peng
Gong Qi
Qingfeng Qi
Xu Qi
Cheng Qian
Guangkun Qian
Wei Qian
Lingling Qiao
Xi Qiao
Yi Qiao
Haoran Qin
Li Qin
Liang Qin
Yongtao Qin
Zhou Qin
Lin Qing
Qihui Qiu
Zhimin Qiu
Shousheng Qu
Bing Rao
Guangbin Ren
Guocan Ren
Lina Ren
Shuyu Ren
Suyi Ren
Tingting Ren
Xiaozhen Ren
Jing Ruan
Na Shan
Shan Shan
Tingting Shan
Lin Shang
Yi Shang
Zeyu Shang
Jian Shao
Jie Shao
MinShen Shao
Yuying She
Lei Shen
Tao Shen
Xiaoxu Shen
Yan Shen
Yang Shen
Yuting Shen
Chengcheng Sheng
Hao Shi
Jian Shi
Jingjing Shi

Kegong Shi
Minli Shi
Pengxiang Shi
Tong Shi
Xiaojin Shi
Miao Shui
Zhengfu Shui
Kunlin Si
Jiahuan Song
Jingyue Song
Liwen Song
Mingming Song
Naishan Song
Shu Song
Yang Song
Meng Su
Shuang Su
Xiaorui Su
Yifei Su
Xiaowen Sui
Congcong Sun
Guihua Sun
Jian Sun
Jin Sun
Li Sun
Lingke Sun
Man Sun
Qianyun Sun
Xinyue Sun
Xu Sun
Yalin Sun
Yan Sun
Yanqiu Sun
Yizhou Sun
Yue Sun
Yuewei Sun
Mengying Tan
Shishu Tan
Jie Tang
Jie Tang
Rui Tang
Zhe Tang
Chengcheng Tao
Juan Tao
Yuanyuan Tao
Guoying Tian
Xin Tian
Yuan Tian
Yue Tian
Yuxin Tian
Zeng Tian
Shengzhong Tu
Ben Wang
Chao Wang
Chen Wang
Dan Wang
Dongyu Wang
Feifei Wang
Gang Wang
Gang Wang
Haitao Wang

Hongxuan Wang	Sunyuan Wei	Jiacheng Xuan	Shuxin Yu	Xuan Zhang
Huihui Wang	Wei Wei	Quan Xue	Shuyao Yu	Yansizhuo Zhang
Huiye Wang	Yujiao Wei	Xinlei Xue	Zhengshu Yu	Yaoqing Zhang
Jiaming Wang	Changkuan Wen	Xiongting Xue	Chao Yuan	Yaosheng Zhang
Jian Wang	Jiu Wen	Shujun Xun	Ding Yuan	Yatian Zhang
Jing Wang	So Man Wong	Chengfang Yan	Jiakuan Yuan	Yichang Zhang
Jing Wang	Binzhou Wu	Li Yan	Juan Yuan	Yifang Zhang
Keming Wang	Geng Wu	Meng Yan	Sailei Yuan	Yihong Zhang
Kun Wang	Gengsheng Wu	Xiangyu Yan	Shangcao Yuan	Ying Zhang
Lei Wang	Hangdan Wu	Xiaomin Yan	Wei Yuan	Yipeng Zhang
Lijie Wang	Hao Wu	Xing Yan	Junlong Yue	Yiwen Zhang
Limin Wang	Hongkun Wu	Yizhu Yan	Yao Yue	Yongxu Zhang
Limin Wang	Jincai Wu	Bei Yang	Yiyi Yue	Yu Zhang
Lin Wang	Jingwen Wu	Bo Yang	Jianchao Zang	Yue Zhang
Lu Wang	Lei Wu	Congyu Yang	Chubin Zeng	Yunyun Zhang
Lujiao Wang	Ming Wu	Danli Yang	Hui Zeng	Zhen Zhang
Manxia Wang	Qian Wu	Dian Yang	Shengnan Zeng	Zheng Zhang
Meng Wang	Weiping Wu	Fan Yang	Xinliang Zeng	Zhuo Zhang
Qi Wang	Wenjie Wu	Haiwen Yang	Ying Zeng	Zida Zhang
Qing Wang	Xiao Wu	Haiyan Yang	Yueqing Zeng	Chen Zhao
Qiong Wang	Xintong Wu	Jin Yang	Jingmei Zha	Cheng Zhao
Run Wang	Xuefei Wu	Jing Yang	Weiyang Zha	Jun Zhao
Runxiao Wang	Xuefeng Wu	Lan Yang	Fangyuan Zhai	Lubin Zhao
Shengxia Wang	Yali Wu	Lei Yang	Xu Zhai	Min Zhao
Shuangliang Wang	Yanxuan Wu	Li Yuan Shako Yang	Boyan Zhang	Ruoqu Zhao
Shuangshang Wang	Yingqi Wu	Ming Yang	Chunyue Zhang	Shaobo Zhao
Shukai Wang	Yuchen Wu	Na Yang	Di Zhang	Shiqin Zhao
Shuo Wang	Yue Wu	Rui Yang	Feifei Zhang	Tong Zhao
Siyuan Wang	Yuhan Wu	Shuhui Yang	Haobo Zhang	Xiaomin Zhao
Songli Wang	Zhiheng Wu	Weihua Yang	Huihui Zhang	Ying Zhao
Sulan Wang	Xiaofei Xi	Xiaouu Yang	Jun Zhang	Yining Zhao
Tao Wang	Lifang Xia	Xiaoting Yang	Kun Zhang	Yongtian Zhao
Tianfei Wang	Yue Xia	Xiaoying Yang	Kun Zhang	Yu Zhao
Ting Wang	Jie Xiao	Ximin Yang	Lei Zhang	Yue Zhao
Wei Wang	Lili Xiao	Xuejiao Yang	Li Zhang	Yuzhong Zhao
Weitao Wang	Tianyi Xiao	Yan Yang	Lin Zhang	Zhenguo Zhao
Wen Wang	Tingting Xiao	Yangyang Yang	Ludan Zhang	Zhifang Zhao
Xiaohong Wang	Yao Xiao	Yi Yang	Luxi Zhang	Qijun Zheng
Xiaolu Wang	Yuqiu Xiao	Ying Yang	Meng Zhang	Ru Zheng
Xinyu Wang	Zhiying Xiao	Yunying Yang	Mengfei Zhang	Xiyu Zheng
Xu Wang	HaiHan Xie	Zhaoyu Yang	Mengmeng Zhang	Yadong Zheng
Xueying Wang	Hengyu Xie	Dan Yao	Min Zhang	Yanbin Zheng
Yanan Wang	Mingxi Xie	Qingyuan Yao	Muqiao Zhang	Yanhua Zheng
Yanzhu Wang	Shenwei Xie	Huanhuan Ye	Ning Zhang	Yashan Zheng
Yating Wang	Shuting Xie	Jingjing Ye	Ning Zhang	Yinglan Zheng
Yi Wang	Tuoli Xie	Xinru Ye	Pinghua Zhang	Yuzhen Zheng
Yicheng Wang	Yiling Xie	Ying Ye	Qian Zhang	Ziyin Zheng
Yidan Wang	Guangyan Xing	Chenxing Yi	Qiang Zhang	Sheng Zhong
Ying Wang	Jing Xing	Fei Yin	Qing Zhang	Xiaofen Zhong
Yining Wang	Cong Xu	Xin Yin	Qiuling Zhang	Ying Zhong
Yiwen Wang	Di Xu	Yan Yin	Renchi Zhang	Donghui Zhou
Yongjin Wang	Fei Xu	Zhen Yin	Rui Zhang	Fang Zhou
Yue Wang	Huimin Xu	Zhidi You	Ruiping Zhang	Han Zhou
Yuou Wang	Humei Xu	Changrong Yu	Sheyu Zhang	Huiqin Zhou
Yupei Wang	Jiayi Xu	Dongli Yu	Tingting Zhang	Jianhua Zhou
Yuqi Wang	Jie Xu	Hang Yu	Wei qi Zhang	Jie Zhou
Zhen Wang	Jingcai Xu	Hong Yu	Wei yi Zhang	Lijuan Zhou
Zhen Wang	Linxia Xu	Jinlong Yu	Xiaobin Zhang	Mengyan Zhou
Zhuqing Wang	Ruixin Xu	Lijuan Yu	Xiaomeng Zhang	Ming Zhou
Ziwen Wang	Wei Xu	Miao Yu	Xin Zhang	Na Zhou
Jingwei Wei	Xin Xu	Min Yu	Xinyi Zhang	Rui Zhou

Xin Zhou
Xinyun Zhou
Xizhi Zhou
Yan Zhou
Yaxin Zhou
Ying Zhou
Yingzhe Zhou
Yingzi Zhou
Yongsheng Zhou
Yu Zhou
Yujiao Zhou
Chonghe Zhu
Hui Zhu
Jiangning Zhu
Jingyi Zhu
Li Zhu
Lingling Zhu
Mengjing Zhu
Shengnan Zhu
Wanlong Zhu
Yadi Zhu
Yining Zhu
Yongbo Zhu
Zhengpeng Zhu
Yufei Zong

Colombia

Jose Eduardo Rojas
Kimberly Suarez-Contreras

Côte d'Ivoire

Cyriaque Towanoun Hounsa

Croatia

Anton Kohut
Maja Kovač

Cyprus

Marina Agathangelou
Kalia Charalampous
Theodoros Stavrou

Czech Republic

Marek Bocanek
Petra Capkova
Gabriela Kindlova

Denmark

Charlotte Rose Lowry

Egypt

Yousri Mounir L. Showeitar

Estonia

Evelin Ruus

Finland

Lisa-Maria Altenberger
Karola Koivula
Wilhelm Lindstrom

France

Natacha Cheron
Caroline Lisiecki
Geraldine Martinez
Florent Paris
Guillaume Riès
Hind Riouch
Julien Winternheimer
Yahui Xie
Pierre Zennadi

Germany

Mahshan Ashouri
Jens Berke
Greta Bortkeviciene
Patrizia Zoi Dafulis
Sylvia Gisa
Ted Hadjisky
Sarah Heller
Marion Hientz
Sheng Jin
Charles Steven Lamb
Eunyoung Lee
Wieland Markert
Marcel Pohl
Norman Todd
Hans-Georg Philipp Treuner

Ghana

Lilian Danso Affum
Langtertaa Karbo
Enoch Kofi Koranteng
Samuel Osei Kofi Kyeremeh

Greece

Zinon Chatziantonoglou

Guyana

Chandan Kumar
Melissa Tashana Smith
Faith June Taylor

Honduras

Gerardo I. Midence Zúniga

Hong Kong

Asif Ahmad
Mak Chun Wai Billy
Siying Cai
Chi Tsun Chan
Ching Yin Chan
Choi Yee Chan
Ka Man Chan
Sai Po Chan
Ting Yiu Chan
Wing On Chan
Yin Cheuk Chan
Yuen Ying Chan
King Shan Chau

Siu Tin Chau
Wai Ning Winnie Chee
Lai Sum Cheng
Zehui Cheng
Ka Yee Cheung
Lok Yee Cheung
Sze Sze Tess Cheung
Wai Ling Winnie Cheung
Wing Tung Sydnee Cheung
Wai Yin Chick
Wing Chi Remy Ching
Yun Tai Chiu
Tak Ki Derek Choi
Chi Kwan Johnny Chow
Ho Ming Chow
Wing Hei Chow
Amanda Chu
Chung Ting Chu
Ho Yi Chu
Man Wui Chum
Yuen Ying Chung
Xinxin Cui
Jiaying Dong
Jonathan Vincent Galaviz
Celeste Goosen
Richard David Grasby
Dandan Guo
Fariyah Hassan
Qing He
Suet Ling Heung
Chi Him Sonny Ho
Chun Fai Ho
Chun Wa Ho
Ka Wai Ho
Wai Leung Ho
Wing Fung Ho
Yan Ting Ho
Kho Cindy Honggo
Madhu S. Hosmane
Wei Ling Huang
Pik Chi Hung
Tsz Chung Hung
Wing Ki Hung
Vaibhav Surendra Jain
Sasha Kalb
Ka Yan Kam
Kam Chiu Ko
Ting Fung Kong
Lam Lam Kwan
Pui-Hin Basil Kwan
Tak Ching Kwan
Wing Ni Kwan
Chun Hin Kwok
Hoo Yee Kwong
Man Kei Lai
Cheong Lam
Ephraim Lam
Hiu Yeung Lam
Sai Ho Lam
Tsun Fai Lam
Wai Ip Lam

Wai Sum Lam
Ying Chun Lam
Po Shan Geraldine Lau
Ting Ting Lau
Tsz Kwan Lau
Tze Yue Lau
Hoi Yee Law
Yat Kan Law
Chun Yin Lee
Lok Yin Rosalind Lee
Nam Ying Lee
Po Yu Lee
Wing Kiu Rowena Lee
Au Sei Leung
Hing-Wa Leung
Ka Lee Kany Leung
Kevin Leung
Yan Chi Ellen Leung
Ho Yin Li
Jizhao Li
Kin Fung Li
Kin Kei Li
Suet Yee Li
Yi Hong Li
Jun Liang
Shaoling Liang
Jiabo Liu
Wang Ho Lui
Kei Fung Luk
Pui Ling Man
Aurore Marie
Sreya Narayanan
Chun Yiu Jason Ng
Ka Kin Ng
King Hei Ng
Yan Wa Ng
Yuen Chuen Ng
Wun Sze Ceci Ngai
Hyun-seok Oh
Si Wan Poon
Jingjing Qiang
John Rinold
Yiu Yeung Ser
Kin Lok Danny Shiu
Hiu Ting Sin
Wing Yin Sin
Chi Ho Siu
Sze Kit Alan Siu
Paul So
Wai Miu So
Amit Soni
Andrew Sprake
Tsz Yan Tam
Carmina Wing Man Tang
Tsz Chun Tang
Wing Hung Tang
Kin Hang Tsang
Kin Ming Tsang
Ka Lai Wan
Tsz Hin Wan
Tiancheng Wang

Chee Weng Wong
Cheuk Gi Churchill Wong
Fung Yee Wong
Hei Ning Wong
Hoi Shing Wong
Ka Yu Rico Wong
Miu Sheng Wong
Pik Ki Wong
She Wah Wong
Shuk On Wong
Tik Man Wong
Tsz Wing Wong
Yan Ho Wong
Yiu Kai Wong
Yuk Lam Navy Wong
Chi Kwong Woo
Hiu Wing Woo
Hei Man Wu
Odelia Hew Tung Wu
King Leung Andy Yau
Chun Hoi Yip
Samuel Wai Keung Yip
Wai Tai William Yip
Cheuk Yin Yiu
Wai Shan Yiu
Ka Man Yu
Pik Tsz Yu
Chuen Ho Yuen
Kin Ming Yuen
Kwun Lok Yuen
Yi Lam Yuen
Jingxuan Zhang
Lulu Zhang
Qi Zhang
Yanka Zhang
Haomiao Zheng

Hungary

Renata Fejes Ujváriné
Richárd Katona
Zsolt Korosi
Tamas Levai
Tibor Racz

India

Mrutyunjaya Acharya
Hussein Attari
Mahalakshmi Ayyasamy
Archana B V
Harshita Bajaj
Paresh Chandra Barik
Manoj Kumar Batra
Usha Amarnath Bhardwaj
Ratna Borse
Navaneeth Chanolian Poyil
Mobin Cherian
Venkata P. R. R. Chintalapati
Venkata Aditya R. Choppa
Kangkan Das
Roopal Dev



TAKE THE FIRST STEP

Join our new community of certified associate professionals, for those earlier in their career in KYC/CDD, transaction monitoring and AML FinTech Compliance.



Start your journey at www.acams.org



Deepthi Dominic
Nitin Mahendra Ganatra
Fezan Gauri
Priyanka Giri
Premdeep Godara
Abhinandan Goswami
Nitin Kumar Gupta
Poorani Ilango
Anurag Jain
Smriti Jajodia
Jiten Shivram Joshi
Pranav K
Vinod Karade
Rinku H Katharia
Mehnaz Khushtar
Suresh Kothandan
Arun Kumar
Premraj Meena
Madhumita Nag
Jebi Numbipunnilath
Susmita Parankush
Divya K Raj
Rajkrishnan Rajan
Jagdeep Singh Randhawa
Kavya Rastogi
Puja Roy
Sandeep Dilip Ruparelia
Akshara Sunil Sawant
Nikita Shah
Mohd Shareef
Ramanuj Sharma
Rinos Banu Sheik Alavudeen
Ramesh Singh
Krishna Solapnor
Mithunkumar M. Surpur
Karan Tambe
Bhumi Nitin Trivedi
Leonidas Tsismetzoglou
Neethu Vattolli Kumaran
Ravin Vyas
Vishwanath Yelkal
Prakriti

Indonesia

Febrina Aruan
Anthoneus Ismoyo Djati
Candra Putra

Ireland

Eleanor Aspell
Daniel Jose Diaz Rey
Emma Gorman
Shane P. Quinn
Tatiana Aparecida Silva
Orla Stockdale
Katie Walsh

Israel

Nevo Lapidot

Italy

Nicoletta Grilli
Alessandro Andrea Miragoli
Alessandra Vitale

Jamaica

Leshana Campbell
Natalie Lotoya Forrester
Carlene Johnson-Saunders
Monique Lawrence

Japan

Meitetsu Emori
Satoshi Hamamura
Masaaki Hara
Rui Hirose
Koji Hisanabe
Toshiaki Hoshi
Aya Igarashi
Yoshitaka Ikeda
Yuko Imada
Yasuko Imura
Hiroyuki Inakazu
Kensuke Kasugai
Chihiro Kawakami
Fumi Kawakami
Tomohiko Kimura
Makoto Koga
Kimihito Kojima
Masashi Konno
Mitsuhiro Kurosaki
Taro Matsuoka
Natalie Mayumi
Sadahiro Miki
Takashi Miyamatsu
Go Mochimatsu
Tomoko Mogi
Takashi Mori
Masato Morisaki
Tomoka Nakamura
Ippei Nakane
Kazuki Niimura
Yoko Nitta
Jiabao Ren
Yoshikazu Saito
Kenjiro Shima
Ryotaro Shimizu
Misato Susaki
Keiji Suto
Maiko Takeuchi
Tomoki Tamura
Nobuhiko Tanaka
Saiko Terada
Mitsuko Yamamoto
Meiko Yamauchi
Atsushi Yasuda
Makoto Yoshida

Kazakhstan

Gaukhar Akina

Kenya

Nicholas Kiptoo Bett
Naomi C. Kipsang
Domitilla Wanjiku Kiragu
Enock Olando Mukabi
Zachariah Magoka Oburi
Bernard Ogake Ogendo

Kuwait

Jenan Alabdulrazzaq
Abdulaziz Ali Almondi
Ahmed Yasin Mohamed
Udit Wadhwa

Latvia

Olga Barča
Janis Mellups
Natali Sorokina
Olga Tumule

Lebanon

Vanessa Chamoun
Antoine Salame
Farid Zebib

Lithuania

Alina Cibulskė
Kristina Gudaite
Vytautas Mockus
Deivydas Razminas
Diana Urbonienė

Luxembourg

Laurent Dao
Giedrius Drulia
Feng Du
Luis Esparza
Cristina García Berenguer
Sybille Giriens Rakintsev
Galit Goldman-Malka
Yadie Li
Andrés Santamaría Alvarez
Maria Isabel Carolina Vago
Siwei Xiong
Xin Zhao

Macao

Carmen Ao
Yong Chen
Ngan Hou Cheong
Ut Sin Chong
Huimin Huang
Iat Kuai Cecilia Lam
Cheng Lam Lei
Nga Weng Lei
Sok Cheng Lei

Man I Leong
Madalena Lo Pino
Raquel Mak
Chi Chong Abilio Pun
Ut Hong Pun
Yun Qian Su
Sut Nga Tang
Kin Keong Tong

Malawi

Tisunge Tiwonge Phiri

Malaysia

Mogan Chandaran
Guan Yu Ng
Nurhidayah Binti Abdul Razak
Poh Cheong Seow
Chin Leong Tsai

Malta

Margherita Alessandri

Mauritius

Gowree Roopnah-Dusoruth

Mexico

Federico Cano Robert
Manuel Arturo Vazquez Torres

Namibia

Menfret Melk

Netherlands

Tolga Aksoy
Kay Al
Roy William Bottenberg
Aimee Brouwers
Suruchi Gawde
Haci Izci
Hüseyin Keyik
Lonneke Kuilboer
Anran Li
Feng Li
Moniva Martina
M. J. Mertens
Kosara Petrova Mihaylova
Gabriela Muñoz Arenas
Riza Can Ozturk
Amelie Schuler
Runbo Si
Ailin Song
Dolly Sabrina Tolesano
Kasım Emre Türk
W. R. S. van de Steeg
Piet-Hein van Zijl
Liudmila Vegter-Boroshko
Emily Verwaal
Marcin Wasilewski
Daehan Wi

New Zealand

Kit Chiu
Louise Coad
Charis Danieli
Md Shafiul Azim Faruqui
Kannitha Kaing
Christelle Launay
Lucas Joseph Mansell
Warden Tamuka Nyawo
Owen Bruce Turner

Nigeria

Taiwo Adeniyi
Olufunke Ajani
Bright Chinweotuto Anyanwu
Ajibola Sunday Fakorede
Abisola Gbadebo
Adefunke Ibrinke
Unoma Ebelechukwu Ndulue
Uchechukwu A. Nwosu
Adeyinka Adeola Oladepo
Olohitare Omomofe
Egundoyin Ajini Oni
Titilope Oluwakorede Rotimi
Clara Idaoerefama Umanah

Norway

Asia Chernova
Runar Nilsen

Oman

Hawraa Al Harthi

Pakistan

Eitzaz Ali
Shehzad Firdous Ali
Prem Kumar
Asif Naaem
Kamran Shahzad
Priya

Panama

Helene Tison

Paraguay

María Teresa González Fretes
Oscar Ramon R. Melgarejo

Peru

Ingrid Del Solar
Armando Martin G. Vasquez

Philippines

Kristine Dela Rosa Candelaria
Mary Grace Jativa
Jerry Labaguis Leal
Blesilda Anne B. Lubag
William Russel Surla Malang

Imelda A. Mifa
 Maria Cecilia G. Natividad
 Jayvee Roca
 Ian Kimmy Tin
 Ramon C. Lazp Viado

Poland

Radoslaw Jastrzab
 Piotr Tadeusz Landowski
 Andrzej Lenartowicz
 Jan Lutze
 Panagiotis Mallios
 Anastasiia Matros
 Tetiana Vorobiova

Portugal

Flavio R. Erreria

Puerto Rico

Gloriel Mercedes A. Colon
 Ivonne Avilés Domenech
 Jorge M. Rivera González
 Evan Turner

Qatar

Ali Warsam Abdalla
 Arwa AbuHamdieh
 Abdulla Mohammed Al Saadi
 Moza Alkuwari
 Abdelkebir Azzi
 Irene Kay A. Branzuela
 Modhureema Chatterjee
 Carlos Jorge Coelho Ferreira
 Arun Kumar Soman Pillai

Russia

Vladislav Anadikt

Rwanda

Ubaldo Sesonga

Saudi Arabia

Essam Abdullah M Al Nasayn
 Abdulrahman K. Alruwaished
 Ibrahem A. Bin Rasheed
 Mohammad Fareed Fatani
 Emtenan Hajar
 Ammar A. Jeddawi
 Zohaib Ali Zahid

Singapore

Jing Hao Ang
 Qi Hui Ang
 Bee Huay Joelle Aw
 A Abdul Basith
 Tajudeen Benazir
 Souvik Bera
 Edwina Ai Leng Chai
 Qing Yuan Chan

How Cher Kayden Chang
 Sai Chuen Chee
 Marcus Qiliang Chen
 Vincent WenDa Chen
 Xinyi Charmaine Chen
 Yongquan Chen
 Jie Yi Cheng
 Wei Jian Clement Cheng
 Hwee San Jessica Cher
 Wei Ling Nicole Chern
 Steven Cheung
 Shi Jie Chew
 Wei Bin Stephen Chew
 Yi Ling Vanessa Chew
 Jia Cheng Chia
 Sin Hung Chia
 Satish Kumar Chilamkurthy
 Han Yi Chim
 Shi Min Charmaine Chong
 Shong Kai Mason Chou
 Hui Hong Daphne Chua
 Mei Na Chua
 Ka Tsun Joshua Chung
 Ong Guo Wei Desmond
 Chinmoy Dey
 Si-Qiang Ronald Ding
 Seah Eng Chye
 Jing Jing Joy Gan
 Wai Yee Sarah Gan
 Kiang Kiat Goh
 Mun Lin Doreen Goh
 Zhi Wei Leonard Goh
 Jie Ying Han
 Qiaolin Han
 Wenting He
 Xinni Daphne Heng
 Chu Hong Ho
 Hwee Cheng Christine Ho
 Wei Lik Ho
 Xin Yi Jaslyn Ho
 Audrey Hoa Zimmel
 Chen Hong
 Yin Lin Jacqueline Houg
 Guan Jie James Huang
 Lina Huang
 Peisi Chloe Huang
 Wen Feng Aaron Huang
 Igor Ivanov
 Darren Jolly
 Xiao Pei Kan
 Zhong Ting Zac Kee
 Akshay Avinash Kher
 Onyou Kim
 Kai Shi Kasey Koh
 Lo Min Cheryl Koh
 Xiangrong Kathleen Lai
 Ming Chuan Daniel Lam
 Weijie Jake Lam
 Ze Wei Kenji Lam
 Asyraf Latiff
 Yan Hong Lau

Chew Yeng Hannah Lee
 Weixiong Lee
 Xuan De Lee
 Wan Li Winnie Leong
 Jing Li
 Lei Li
 Mengran Li
 Yongjing Michelle Li
 Hwee Leng Janice Lim
 Jun Wei Gerald Lim
 Nu Yi Rachel Lim
 Weijun Lim
 Yu Feng Lim
 Yuze Lim
 Zi Yun Lim
 Chiao Hsuan Lin
 Daohan Lin
 Siew Fong (Felicia) Loh
 Wei Hao Loh
 Yen Har Josephine Loh
 Yi Sheng Loh
 Zhen Wen Shawn Loh
 Jianhui Low
 Yi Han Elle Low
 Aidalyn De Claro Lualhati
 Whye Mun Jonathan Lum
 Vidhya Madhavan
 Vina Misra
 Tanmoy Mitra
 Khay Mar Myo Aung
 Thulaja Naidu Ratnala
 Cui Shan Rachel Neo
 Boon Tiong Ng
 Han Liong Ng
 Jiehao Ng
 Ng Zi Bryan Ng
 Scott Gabriel Ng
 Su Khay Ng
 Tse Ching Tracy Ng
 Ying Hui Ng
 Wei Chang Ngauw
 Jing Wen Juliene Ong
 Sze Yun Ong
 Xiu Hui Ong
 Rashmi Pabla
 Siak Evelyn Peiyun
 Wen Hui Phua
 Wei Ling Rebecca Poe
 Bowen Qian
 Ying Fang Quek
 Girish Raghavendra Rao
 Ashish Rawat
 Shiew Yi Shi
 Wei Ming Sieng
 Yun Ling Eileen Siew
 Paul H. S. Singh
 Wan Hua Siow
 Xin Yi Sitoh
 Jiayin Song
 Seow Ying Soon
 Yu Fang Soon

Shuang Su
 Thenmozhi Sundaramurthy
 Ah Heng Tan
 Ailing Tan
 Candace Tan
 Fu Ling Casey Tan
 Hong Jun Rachel Tan
 Joslynn Li Chuin Tan
 Kang Yong Alfred Tan
 Kim Hong Alvin Tan
 Mei Yan Tan
 Si Rui Tan
 Tang Lim Heather Tan
 Tze Kye Kenny Tan
 Wee Kiat Joel Tan
 Xiangyun Tan
 Yen Ming Tan
 Yong Da Jason Tan
 Zhi Ming Melissa Tan
 Vishal Taneja
 Zhi Xiang Zax Tang
 Xiangyou Ezra Tay
 Yang Zhi Nicholas Tay
 Xue Bin Teoh
 Arun Thanawala
 Jie Ling Jacqueline The
 Yihua Terence Thien
 Kum Yen Tong
 Vrishali Abhijit Vekhande
 Shi Bin Charlton Wan
 Jingjie Wang
 Shi Yi Wee
 Jing Yu Wong
 Soo Wei Wong
 Wei Xuan Wong
 Chee Wai Samuel Wu
 Jenalynn Jianing Yang
 Chun Woei Yap
 Yeow Boon Danny Yap
 Li Han Jasmin Yeo
 Shang Kun Yeo
 Zhen Hao Yeo
 Thiam Ming Desmond Yong
 Xiaoxin Zhu

Slovakia

Richard Cukovic
 Ing. Petr Hajda

Slovenia

Sebastijan Peterka
 Masa Zalar

South Africa

Jorge Azevedo
 Sharmilla Gajan
 Meganathan Govender
 Shenghua Jiang
 Lawrence Luke A. Kayamba
 Nolene Singh
 Ofentse Alec Theledi

South Korea

Jee Woon Bahng
 Ahn Cheol Hong
 Byeongjun Choe
 Su Jeong Choi
 Yangwun Choi
 Seungjoo Han
 Seungmok Han
 Sung Keun Hong
 Kyung Ok Hwang
 Seokbong Jang
 Da Eun Jeong
 Eun Hee Jeong
 Hee Yoon Jeong
 Dan Kim
 Dong Hyun Kim
 Dongmin Kim
 Geunwoo Kim
 Hoisuk Kim
 Hyo Won Kim
 Jeongin Kim
 Ji Hyang Kim
 Ji Hyun Kim
 Joeun Kim
 Myoungshin Kim
 So Eon Kim
 Sung Yeon Kim
 Woo Jeong Kim
 Young Bae Kim
 Young Sic Kim
 Hyun Ji Lee
 Myungah Lee
 Seonghye Lee
 Hyun Sil Lim
 Ki Hoon Nam
 Jiyoon Park
 Moon Sook Park
 Yoon Young Roh
 Woo Seung Sohn
 Pengyang Wang
 Young Chan Yang
 Seomin Yoon

Spain

Ángela Colás González
 María Freire Pequeño
 Fernando Martín Garmendia
 Viktoria Kolesnikova
 Maria Mateos Junquera

Sri Lanka

Ramith Bandara Ranathunga
 Janani Sriskandarajah

Saint Kitts and Nevis

Keishara C. Liburd
 Mark Mangan

Sweden

Emil Bexenius
 Carl-David Sukrit Lundström
 Hanna Lüttschwager
 Emil Richloow
 Georgette Shinoda

Switzerland

V R Phani Kishore Basavaraju
 Leila Boulkerara
 Gonçalo Cardoso
 Anna Cecere
 Giulio Filippi
 Myriam Fleurdépine
 Maria Carolina Marcondes
 Christian Peiffer
 Paulius Stulpinas
 Roshnee Kiran Thakore

Taiwan

Kuo Chieh Chao
 Hsinyi Chen
 Li-Tang Chen
 Ying Chien Chen
 Ying Mei Chen
 Chun Yu Carey Chien
 Chun-Hui Cho
 Chun-Yao Chuang
 Hsiao Fei Ho
 Huei Shin Hou
 Chia Chen Hsieh
 Ning Yu Hsieh
 Yu-Sheng Hsin
 Yeh-Yi Hsu
 Fong Jia Hu
 Pei Hsuan Huang
 Hsiang-Ting Lee
 Yi Hsing Liang
 I Hsia Lin
 Fang-Chun Liu
 Shu Lin Liu
 Yushan Lo
 Chia-ling Ree
 Shu Chen Shih
 Yen Ping Sun
 Yu Chi Ta
 Chia-Lung Tang
 Yu-Hsuan Teng
 Pei-Chen Tsai
 Hsin Ping Wang
 Yi-Hua Wang
 Tsai-Yu Wu
 Mei Hsien Yang

Togo

Abdoulaye Ibrahim Beidou

Trinidad and Tobago

Kern DeBique
 Anna-Lisa Daldas
 Stacey L. O. Honore
 Natalie Noel
 Kimberleigh Peterson
 D. J.-M. Selman-Carrington
 Antonio Villaverde Areces

Turkey

Ahmet Can Demir
 Caner Kaya
 Engin Simsek

Turks and Caicos Islands

Soreka Sharonda Brown

Uganda

Mugisha Habib
 Kenneth Natukunda

Ukraine

Marta Babyak
 Ivan Paramonov

United Arab Emirates

Sameer Ahmad
 Mamta Ajmera
 Aisha Essa A. Khalfan Al Ali
 Omar Ibrahim Alhasnawi
 Akhtar Ali
 Reem Abdulrazzaq Anwahi
 Hisham Ayamu
 Stebin Chungath Baby
 Ammar Ali Baig
 Ayesha Butt
 Deepti C. Pillai
 Hanee Ali Chanwan
 Sriram Chokkalingam
 Emma Louise Cowan
 Benjamin Crossland
 Nachiketh Deshpande
 Mugdha Mahesh Dhomkar
 Diana Dsouza
 Roma Dsouza
 Sharon D'souza
 Prince Ebbin
 Arish Ehsan
 Lily Eid
 Diala El Zoueinah
 Hanna Joseph Francis
 Melodie Haddad
 Irfan Ullah Ihsan Ullah
 Anubha Jain
 Dilip Jain
 Leroy Mathew Jones

Sushanth K
 Ibrahim Khaleel P. Mohiddeen
 Divya Khiara
 Bharat Khurana
 Vinodh Kooriyattil
 Girish Krishna Shetty
 Mohamed Lafir
 Kumaravelan Loganathan
 Soumya Mathew
 Lloyd Meadows
 Jayesh Meethale Veettil
 Shaimim Meraz
 Anila Mohamed Rafeek
 Nazer Hamzath Mohideen
 Ria Nangia
 Noman Nazim
 Ali Hussain Noorjahan
 Sheetal Noronha
 Ammar H. Aldeen Eid Obeidat
 Chandraprabash P C
 Ajith Chandran Pallath
 Yogita Ajay Panandikar
 Vijish Vijayan Panicker
 Vivek Gokuldas Panicker
 Shakkeel Naduvile Purayil
 Saumya Rajan
 Dala Ram Ram
 Sanjay Ramchandani
 Alok Ranjit
 Rakhisha Rasheed
 Mohammad Rayess
 Syed Asif Raza
 Shuja Ur Rehman
 Vishal Relhan
 Smitha Sadasivan
 Ginu K. Samuel
 Sonali Vijay Sathe
 Pinky Nikesh Sawant
 Trisha Sen
 Sherif Shaaban
 Muhammed Shabinudheen
 Soumya Sharanagowda
 Balwant Kumar Singh
 Srithar Srinivasan
 Savitha Subramanian
 Divya Thanvi
 Abdul Azeez Thayyil Kokkatt
 Keo Akemi Yap Tiong
 Aiden Varghese
 Anu Varghese

United Kingdom

Alimat Oluwatobi Adedayo
 Aramide Akisanya
 Tasmia Akter
 Rimjhim Bijay Kumar
 Sinead Julia Carcavella
 Thomas Davy
 Arianna De Luca
 James Deaville

Nikolaos Drosos
 Sarah Edney
 Aziz El Kaissouni
 Izabella Eninn
 Idriss Imorou
 Rebekah Jones
 Tejasvi Deepak Karnik
 Agnieszka Kerby
 Siar Khoreishi
 Tomas Yago Lafon Ameijeiras
 Nikhil Lavanian
 Luke Louca
 Philip Michel
 Nicola Morgan
 Oluwatoyin Olanpejo
 Femi Mark Olufeyisann
 Charles Edward O'Neill
 Damian Parminter
 Sonia Pereira
 Karol Poplawski
 Jake Nicholas Rawinsky
 Nahilla Razaq
 Elizabeth Reid
 Shruti Revankar
 Najee Riaz
 Vishal Sampat
 Shamaila Shahjahan
 Khalid Sheikh Mohamed
 Loic Sylvain Sienche
 Stuart Philippe Sims
 Ritu Singh
 Rajesh Ramesh Talpade
 Trevor Tanchel
 Carole Turner
 Rita Francesca Valentini
 Monika Visy
 Frances Eve Whittaker
 Yang Yu

United States

Monica Abad
 Ramon Abascal
 Alessandro Abate
 Charles Abuah
 Benicia Acevedo
 Itzel R. Aguirre
 Rahat Ahmad
 Vivien Ai
 Korede Michael Ajileye
 Adenike Olajumoke Akinwusi
 Monica Yalul Alarcon Martinez
 Ashley D. Alimbuyao
 Zack Allison
 Max A. Alves
 Abigail Yeboah Ampratwum
 Bruce Anderson Jr.
 Brian Andres
 Oladayo Anipole
 Feyisayo Aregbesola
 Madilynn Ashworth

Laura Audette
 Ryan Bacher
 Cesar Baez
 Omotola Adesile Bakare
 Jesse Baker
 Nakesha Tania Ball
 Lindsey Barnett
 Jessica Barton
 Kimberly Beckstrom
 Ellie R. Bedford Nowland
 Elena Begunova
 John Kofi Bempoh
 Iana Berger
 Justus Rolf Bieber
 Linus Billings
 Lynda Jean Bird
 Joshua Black
 Chad G. Blanchard
 Jeffery Blossom
 Mitchell Bono
 Camille Bossut
 Graeme Bourne
 Caitlyn Briann Brown
 Mason T. Bruner
 Masayo Bruno
 Ethel C. Buangan-Gee
 Joseph R. Burwell
 Hameed Butu Onakoya
 Courtney Hugh Byles
 Erin Callahan
 Ana P. A. Lopes Campanini
 Carlos Meneses Canales
 Julia Elba Cancino
 Gregory Lloyd Carr
 Huei Chacon
 Iram Chapa
 Saramma Cherian
 Sin Yi (Kaitlin) Cheung
 Linnette V. Chew
 Stephen Chicoine
 Erik Chou
 Imtiaz R. Chowdhury
 Veronica Christy
 Joon Woo Chung
 Benjamin Clinard
 Adam Clough
 Connor Lamar Coleman
 Mary Wallace Coleman
 Matthew Collins
 Nicholas Colón
 Normaliz Colon Ascanio
 Donna A. Colwell
 Shawn Connolly
 Natalie Connolly
 Cesar A. Cortez
 Joseph Cosmides
 Katrina Crider
 Rachel Krenzer Crittenden
 Carlos Cuadra
 Jennifer Lynn Cunningham
 Karl Curry



SANCTIONS SPACE

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



The CGSS
Certification



Online
Training



Masterclass
Series



Monthly
Sanctions
Updates



Thought
Leadership



Networking

Explore these options at
acams.org/sanctions

Anna Cvitkovic
 Janelle Daniel
 Hollie R. Daniels
 Humberto D'ascoli
 Adam John Daufen
 Shivam Rakesh Dave
 Dave Dawson
 Coretta Jordan De Leon
 Hashani Denawakage Dona
 Heather Deyarmin
 Tracey Diggs
 Courtney Dinardo
 Andrew DiOrio
 Richard Doebele
 Jeffrey Doran
 Krystal X. Dou
 Ciaran Cormac Egan
 Puthenpurakkal S. Elizabeth
 Julianna Elyse Ennamorati
 Lorena Esparza
 Steve Estevez
 Yan Fang
 Christian Fernandez
 Zachary Fontes
 Kaitlin Fox
 Yana Galitsyna
 William Galton
 Fabiola Garduño Velázquez
 Jason Garverick
 Clark Sherman Gascoigne
 Brian Gelbert
 Imisi George
 Katherine Gillett
 Nicole Givens
 Miron Goldgeil
 Jose Gomez
 Sandra Gomez
 Manuel Gonzalez
 Hubert Grabowski
 Sheila Lynn Gray
 William C. Gray
 Crystal Green
 Jeff Grimes
 Erik Grossman
 Lauren Elizabeth Grzyboski
 Jose Luis Guerra
 Jenna Guerriero
 Jared E. Guthrie
 Andrew J. Gutshall
 Glenna Hagopian
 Syed Aftab Haider
 Meagan Hailey
 Ericka Hallgren
 Siobhan Delaney Hanlon
 G M Nurul Haque
 Nicole Harlan
 Andy Harley
 Mayra Harmon
 Cheryl Harris

Preston Haxo
 Evan Warner Henderson
 Lisa Heuring
 Jennifer Hicks
 Alison Hinds-Pearl
 Preston Holyfield
 Elise Diamond Howard
 Anthony S. Hrestak
 Kai-Ju Hu
 San Huang
 Jordan Hudspeth
 David Hunn
 Takahiro Ito
 Lyndsey Camille Jackson
 Valerie Jackson
 Robert Jahanfar
 Anisha Jain
 Jennifer James
 Neal Johanson
 Carlos M. Johnson
 Gianna Johnson
 Thomas Scott Johnson, Jr.
 Brandon William Jones
 Cylenthia Drinkard Jones
 Amrita Vijay Joshi
 Namita Karunakaran
 Anna Elizabeth Kasparek
 Asher Keam
 Valeria Brukhis Kennedy
 Sumer S. Khadra
 Sameer Khale
 Sajjad Kamal Khan
 Sang Yup Kim
 Hilary Klein
 Dorota Kobik
 Jonathan R. Koffmann
 Oleg Korets
 Jayson Kowiak
 Dilyana A. Krasteva
 Aaron Kruger
 Erik Krusch
 Kendra Kubin
 Felix Y. Kwan
 Iryna Kyryliuk
 Wendy Lynn Lambach
 Ryan Mitchell Landin
 Luis Lara
 Christa Lasher
 Joseph LaSpina
 Jeffrey Lauer
 Alina Laumann
 Patricia Leary
 Hye Jin Lee
 John Y. Lee
 Mariya Leonova-Jones
 Nancy Halpern Lesser
 Ka Man Li
 Eui Kyung Lim
 Maria Lindstrom

Sarah Lohschelder
 Diana V. Londono
 Mark Alfred Loucas
 Joseph Lounds
 Angus P. Lowe
 Chun Lu
 Timothy L. Lukavsky
 Brandon Luth
 Norman Ly
 Kathryn Lynn
 Louisiane Maciel
 Yonique Malbranche
 Austin Maney
 Gohar Manukyan
 Justin Margolis
 Keith Martell
 Elias L. Martinez
 Makayla Martinez
 Pedro A. Martins Coias
 Alex Masbruch
 Perry D. Mastrocola
 Siewhiang McCreight
 Ronak McFadden
 DeAngelina McGee
 Lola McKindles
 Stephanie McNeely
 Valeria B. Melincu
 Hannah Elizabeth Melot
 Carlos Mendez
 Ptoshia K. Merrills
 Elise Messerli
 Ibrar A. Mian
 Leyla Milman
 Laura Minnick
 Anna Rose Mobilia
 Craig Thomas Momberg, Jr.
 Keion Morgan
 Kristen Kyle Morgan
 Anne Moscato
 Kelly Margaret Moyes
 Shreya Mozumder
 Vance Murphy
 Michael C. Nelson
 Terehas Nelson
 Samuel John Njoku
 Gaddiel E. Nkrumah
 Pamela A. Nkwocha
 Lucy Nzei
 Ndidi C. Obicheta
 Lauren O'Brien
 Henry Ododah
 Sakine Oezcan
 Jacqueline Ogden
 Julien Ogden
 Muiyiwa Ogunjobi
 Olumide John Ogunjobi
 Scott OKeefe
 Nancy Olguin
 Brady Olson

Catherine Orfanos
 Suzi Isedua Oriafio
 Michelle Osofsky
 Simon Alexander Ospenson
 Julie Paben
 Suzanne B. Panagopoulos
 Cueme Parker
 Gregory D. Pashayan
 Hiral Patel
 Herbert Pau
 Andre Payan
 Rui Pereira
 Kelbi Perkins
 Jamie Pfanstiehl
 Cesar Pineda Contreras
 Michele L. Pitta
 Lilliana Posada
 Christian Presto
 Scott Preston
 Suman Priya
 Mingming Pu
 Gina Pye
 Jennifer Ragsdale
 Kennedy Reed-Hoster
 Amie Reilly
 Leah Reitmeier
 Maria Belen Revel
 Hector M. Reyes
 Mochamad Reza
 Chanay Richardson
 Shimon Richmond
 Heather N. Riley
 Ariel Rivero
 Sharmaine D. Robergeau
 Jarrett Miles Cash Robinson
 Sandra Roever
 Veronica Roman
 Caesar Romero
 Steven A. Rosen
 Alex Ross
 Danielle Rowekamp
 Amanda Marie Salasek
 Luke Salyer
 Adriana Sanchez
 Sylvia Sanchez
 Hari S. S. Venkatachalam
 Ean Schmitt
 Ryan Michael Schobert
 Jesse David Scouler
 Nathan Segal
 Dea Semini
 LeShell Session
 Vijay Shanker
 Andy Shanks
 Ashutosh Sharma
 Yehia Shelbaya
 James Sheridan
 Christopher Sidler
 Tara Skinner

Jennifer Smith
 Chad Paul Snyder
 Juliana Ugaya Soileau
 Krystal M. Somers
 Jason Soto
 Tristan Souness-Wilson
 Anna O. Stallings
 Mikel Stevens
 Sean Stevens
 William Stewart
 Michele Struckman
 Premkumar Subramanian
 Sunita N. Sugrim
 Joann Tang
 Alyssa Tascione
 Theodore Taylor
 Brittany Teefey
 Zach Tekely
 John Charles Thomas
 Stefan Ozziel Trevino
 Fei Ching Tseng
 Khurath Ul Ain
 Reecha Upadhyaya
 Roy Varghese Varghese
 Cynthia Vasquez
 Susana Vasquez Franco
 Raymond Villanueva
 Bradley Voight
 Robert Voorhis
 Robert C. Vreeland
 Greg Wagner
 Carrie M. Walchko
 Reyn Watanabe
 Jennifer Weinberg
 Claudia Weinstein
 Jonathan Glen Wells
 Hana Wharton
 Christopher James Wheatley
 Antoinette Woolner
 Jason Worley
 Carrie L. Worthington
 Tiantian Xiao
 Jung Eun Yoo
 Justin M. Zavis
 Yihan Zhang
 Crystal Zimmerman
 Renata M. Zloza

Vietnam

Thu Tra Nguyen
 Thao Minh Tran

Yemen

Osama Omer Ali Mohammed
 Hussein A. AlMehdhar

Zambia

Sibeso Mutumweno



CGSS GRADUATES: MAY-JULY

Graduates countries/regions are sorted alphabetically

Armenia

Zaruhi Badalyan

Australia

Say Pheng (Sophia) Foo

Jun Li

Venkatesh Nathilvar

Qiang Sun

Bahrain

Imtiaz Ahmad

Rajnish Ranjan

Muhamad Nizam Bin Shaidon

Bangladesh

Mohammad A. Al Mamun

Belgium

Frederic Jadot

Geoffrey Max Lepage

Canada

Jinhe Li

China

Yu Bai

Ning Bu

Lijuan Cai

Yinzhu Cai

Rui Cao

Yue Cao

Jinxi Chang

Hongwei Chen

Ting Chen

Xue Chen

Seong Hyun Cheon

Anqi Chou

Ruoyan Fan

Huaqiang Fang

Xiangli Ge

Jiayan Guo

Qian Guo

Wenli Guo

Fang Hao

Peng Hao

Keqing He

Yuanwei He

Qi Huang

Wei Huang

Wenjing Huang

Yanbing Huang

Ying Huang

Zhuojun Ji

Ling Jiang

Xia Kang

Beidi Li

Carter Li

Jing Li

Na Li

Pan Li

Rong Li

Wei Li

Yue Li

He Lian

Jing Liang

Juan Lin

Yun Lin

Min Ling

Guanhao Liu

Haonan Liu

Juan Liu

Xiangning Liu

Yanbin Liu

Yitian Liu

Dan Lu

Mei Luo

Difang Lv

Xiao Ma

Ying Ma

Yiwei Miao

Xingkang Ni

Zhiwei Niu

Rui Pan

Jia Qi Pang

Yanmei Pei

Feifei Qiao

Wenjiao Qin

Yifeng Qiu

Yan Ren

Jian Shuai

Bo Song

Kaijun Su

Liting Sun

Jing Tan

Xinwei Tan

Lian Tang

Qi Tang

Zhen Kun Tu

Chen Wang

Hongtao Wang

Wei Wang

Xueping Wang

Yanhong Wang

Yuan Wang

Jun Xia

Jieyan Xiang

Bingchao Xu

Guangda Xu

Yuxue Xu

Xiaoting Yang

Qing Ye

Chuan Yin

Xuan Yin

Min Yu

Yueqing Zeng

Naihong Zhang

Qiongyue Zhang

Wei Jing Zhang

Yilu Zhang

Nan Zhao

Yingjiao Zhen

Shiting Zhong

Qianyu Zhou

Xiaoying Zhu

Denmark

Jeffrey Nielsen

Egypt

Noha Ashraf M. A. Megid

Finland

Mark Bossmann

France

Alberic Botella
Julien Gallo

Germany

Ruiya Fu
Antonio Stoyanov

Greece

Anna Damaskou

Hong Kong

Hau Ying Hollister Chan
Ying Kit Chan
Man Kit Cheung
Wai Lung Chung
Zhenwei Dai
Ting Wai Ho
Bing Hu
Ming Wai Lee
Yuen Shan So
Shing-Yan Tse
Alexey Tyurin
Chi Yin Yau
Aizhen Yu

India

Ravi Chandel
Naveender Singh S
Rohan S Srihari

Italy

Marcella Binda

Japan

Yasuhisa Furuta
Kasahara Kenichiro
Noriko Nakane
Saori Ohira

Muramatsu Osamu
Makoto Sato

Kuwait

John Simon

Latvia

Laura Kalnina

Lebanon

Rita Fares
Khaled Haidar
Myriam Khairallah

Mexico

Tania Balanzario Meraz
Miriam Guillermo Blancas
Benjamin Serra Cruz

Netherlands

Inbal Djalovski
Ruofei Shen
Erdem Tascilar
Annemarie Verkerk

New Zealand

Jatin Kumar Mistry
Rani Pillay
Minyu Zheng

Nigeria

Babatunde Olaoluwa Macaulay

Norway

Eva Helena Deinoff
Eivind Parr Ohme

Pakistan

Nasir Mehmood

Philippines

Frances Lynette Sayson

Poland

Wenbin He

Puerto Rico

Luis Miguel G. Hernández
Natalia Rodriguez

Qatar

Muhammad Shahid Farid
Neil Scully

Russia

Aleksei Andreevich Pana

Singapore

Alkhaff Akthar
Ming Quan Wesley Ang
Qiyang Kenneth Boey
Sau Young Chung
Vijay Gopaladesikan
Weiliang Hu
Janet Gek Lang Low
Soon Hwee Tee
Sok Mun Wan
Raymond Wong
Siew Peng Woo
Xiaoqian Zhao

South Korea

Dongyeop Hyun
Ping Ji
Jaekyung Kim
Jeongeun Park
Zongrui Yin

Switzerland

Xavier Charles Didier Béard
Aliaksandra Hurynovich

Taiwan

Chih-Feng Chung

Turkey

Melik Bagis Bilici
Bilal Ertogrul

United Arab Emirates

Monqez Alrass
Jamie Belino
Jyoti Das
Asmaa Youssef Ali Elalawy
Gurminder Harinder Singh
Amritha John
Amit Kumar
Suranga Buddhike Marcus

Rasha Mortada

Rima Mourad
Sudhakar Sanjeevi
Michael Wong

United Kingdom

Jane Alimonda
Julie Choudhury
Clare Anne Davies
Monica Handoo
Kevin Penter
Mark Sallis

United States

Julio Gabriel Borrás
S. A. L. Broekaart-Hjalber
David Cellante
Alexander Chan
Bin Chi
Harry Paul Cupp
Michelle Alexandra Dominguez
Terence Egan
Sam Adam Elnagdy
Eva Errico
Jiang Q. Huang
Clara Kim
Elizabeth A. Larson
Laura Larson
Jianyu Li
Lin Li
John Victor Medina
Dimitri Michaloutsos
Aya Muto
Sissy Maite Oliver
Yiqiong Pan
Francisca E. Peralta
Steffy Shaji
Eugenia Shraga
Diana Sirila
Michael A. Tooshi
Bieu Bu Tran
Yu Xu



Go Beyond Your CAMS Credential



The Advanced CAMS-Audit Certification

is an advanced specialist level certification, designed for those conducting AML audits, and other professionals involved in the independent testing of Anti-Financial Crime controls.

Find out more

www.acams.org/cams-audit



Superior customer experience

10X FASTER RESPONSE TIMES



meets



Superior employee experience

80% LESS MANUAL WORK

with **Intelligent Automation.**

 **WorkFusion**

Your team is capable of more.