ACAMS® TODAY

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

Artfully done

Deconstructing a fraudster

SEPTEMBER–NOVEMBER 2017
VOL. 16 NO. 4

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

www.ACAMS.org
www.ACAMSToday.org

ACAMS® | Certificates

Convenient, online, mixed-format training for compliance teams of all sizes ranging from early to intermediate career levels.

Transaction Monitoring

Trade-Based Money Laundering

Cyber-Enabled Crime

Sanctions Compliance

KYC CDD

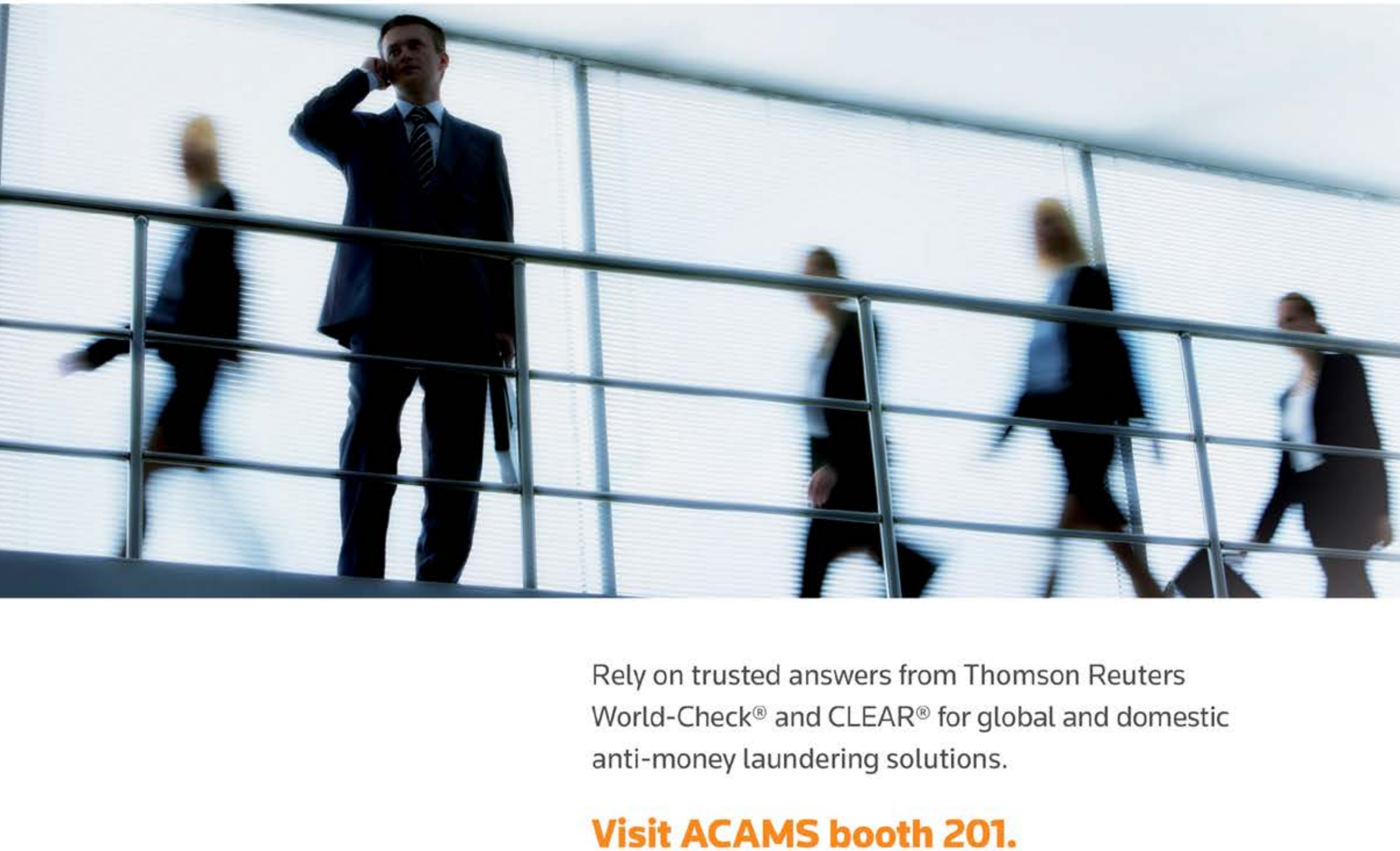
Counter-Terrorist Financing (CTF)

AML Foundations

Participants who successfully complete ACAMS Certificate courses receive:

- A certificate of completion proving their commitment to protecting their institutions against money laundering, terrorist financing and other financial crimes.
- Four CAMS credit hours to keep them on track towards CAMS certification or CAMS recertification.

Earn your training certificate: **acams.org/certificates**



ACAMS® TODAY

EXECUTIVE VICE PRESIDENT *John J. Byrne, CAMS*

EDITOR-IN-CHIEF *Karla Monterrosa-Yancey, CAMS*

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

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

Tel. 1-866-459-CAMS (2267)
or 1-305-373-0020
Fax 1-305-373-7788
Email: info@acams.org
Websites: www.ACAMS.org
www.ACAMSToday.org
Twitter: @acamstoday

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

| SENIOR STAFF |

PRESIDENT AND MANAGING DIRECTOR *Tim McClinton*
HEAD OF ASIA *Hue Dang, CAMS-Audit*
SENIOR DIRECTOR OF OPERATIONS AND CUSTOMER SERVICE *Pierre-Richard Dubuisson*
VICE PRESIDENT OF SALES *Geoffrey Fone, CAMS*
HEAD OF EUROPE *Angela Salter*

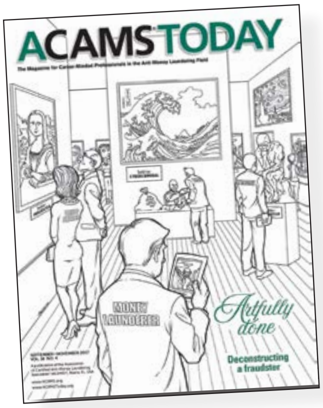
| SALES AND REGIONAL REPRESENTATIVES |

SENIOR VICE PRESIDENT OF BUSINESS DEVELOPMENT *Geoffrey Chunowitz, CAMS*
HEAD OF GLOBAL ACCOUNTS *Sonia Leon, CAMS-Audit*
HEAD OF AFRICA & THE MIDDLE EAST *Jose Victor Lewis, CAMS*
HEAD OF CARIBBEAN *Denise Perez, CAMS*
DIRECTOR OF SPONSORSHIP & ADVERTISING DEVELOPMENT *Andrea Winter, CAMS*

Contents

About the cover: This edition highlights the perplexing issue of money laundering in the art market. Take time to de-stress and color the *ACAMS Today* cover! Send an image of your colored-in cover to editor@acams.org or to @acamstoday.

Illustration by: Jason Robinson



ON THE COVER:

Engulfed by a masterpiece

Last year I had the opportunity to visit the Musée de l'Orangerie in Paris. I have visited this city on numerous occasions, but I have never made it to l'Orangerie, despite the fact that this museum houses several important works by impressionist artists, which is my favorite genre of art. Among these works is Claude Monet's masterpiece, the *Water Lilies*. Monet helped design the museum with the intention of providing the best viewing conditions for the *Water Lilies*. There is a series of interconnected oval-shaped rooms with Monet's compositions hung wall to wall against the long axis at either side of each room. As I walked into the *Water Lilies* exhibit, I truly felt what Monet said about his painting, it creates the "illusion of an endless whole, of a wave with no horizon and no shore." As I turned slowly around to take in every inch of the room, I was suddenly engulfed in his masterpiece.

As financial crime prevention professionals, we too, can sometimes be suddenly engulfed by the demands of work or by the new challenges that this wonderful, exciting yet challenging field has to offer. As such, our masterpiece becomes solving the financial crime. The headline article *Artfully done* sheds light on an area where criminals are polluting something beautiful, such as art, and using it to launder their ill-gotten gains. Is more regulation needed in the art world? Discover what can be done and what the community as a whole can do to fight this emerging challenge.

Our next headline article takes a deeper dive into the financial crime prevention masterpiece. *Deconstructing a fraudster* helps us understand the mindset of a fraudster through developing detective and preventive measures.

Continuing with the dissecting of our masterpiece, the article *Attracting compliance talent* shows you how to attract, retain and develop the best AML professionals to help grow and improve your organization.

This issue is filled with many more articles to help any financial crime prevention professional in their daily job, but I am excited to share with all of you two interviews contained in this edition. I had the great honor of visiting Homeland Security Investigations (HSI) El Dorado Task Force (EDTF) and spending the day with several team members who shared their war stories and I even interviewed an undercover agent. HSI EDTF is celebrating 25 years of fighting crime. In addition, we have an in-depth interview with two of our Advanced Certification graduates, Lauren Kohr and Jack Sonnenschein, who share their experiences and knowledge about obtaining their Advanced Certifications.

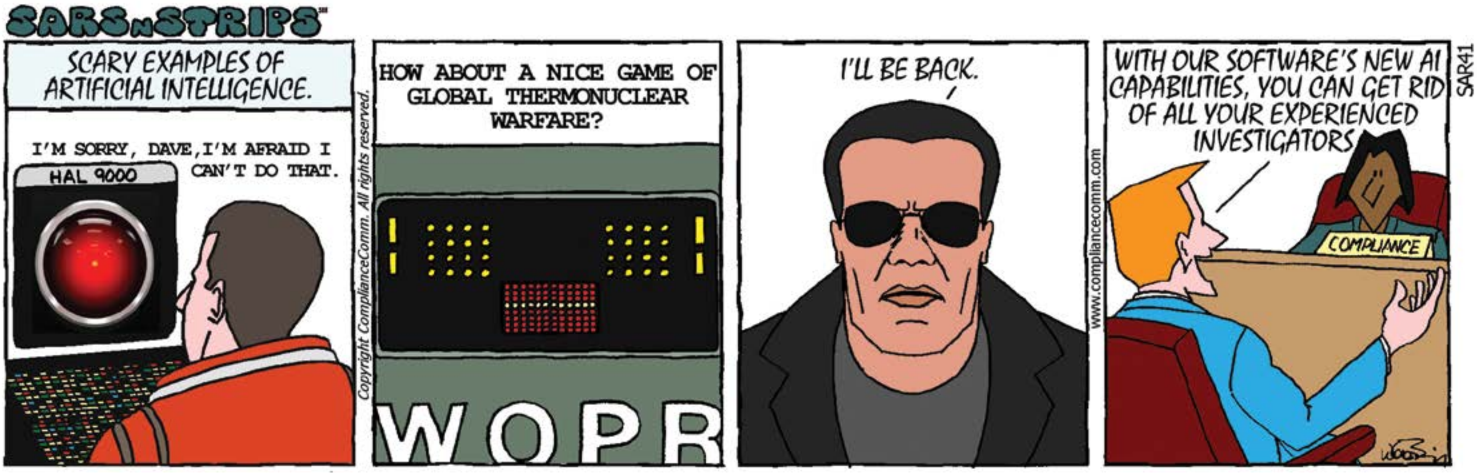
Also, *ACAMS Today* is now on Twitter, so be sure to follow us @acamstoday for the latest updates, articles, happenings and much more.

Finally, I would like to take this opportunity to thank John J. Byrne for his many years of service and commitment as ACAMS' executive vice president. His leadership, mentorship and numerous contributions not only to ACAMS, but also to the entire financial crime prevention community cannot be overstated. John, we know that as you continue to transition more into teaching, writing and speaking we will still continue to benefit from your knowledge and expertise in the financial crime prevention field.

Thank you, John, for your leadership.

Karla Monterrosa-Yancey

Karla Monterrosa-Yancey, CAMS
editor-in-chief


SARSnSTRIPS™
SCARY EXAMPLES OF ARTIFICIAL INTELLIGENCE.
I'M SORRY, DAVE, I'M AFRAID I CAN'T DO THAT.
HAL 9000
Copyright ComplianceComm. All rights reserved.
HOW ABOUT A NICE GAME OF GLOBAL THERMONUCLEAR WARFARE?
WOPR
I'LL BE BACK.
www.compliancecomm.com
WITH OUR SOFTWARE'S NEW AI CAPABILITIES, YOU CAN GET RID OF ALL YOUR EXPERIENCED INVESTIGATORS
COMPLIANCE
SAR41

Produced by: ComplianceComm

WHERE HAS YOUR ACAMS TODAY BEEN?

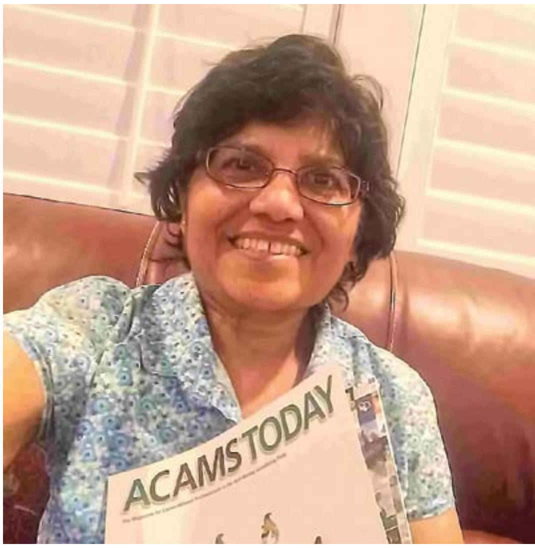
Vasu Sanghani with her March-May 2017 edition of the *ACAMS Today* at a Starbucks coffee shop in Walnut Creek, California.

Kaluwa Maitre-Avril spotted with the Seventh Law Enforcement edition of the *ACAMS Today* magazine at the *12th Annual AML and Financial Crime Latin American Conference* in Cancun, Mexico.

Todd Beck snags a quick picture at the Gorkhi-Terelj National Park in Mongolia with his copy of the December 2016-February 2017 *ACAMS Today* magazine.

The **HSI El Dorado Task Force** poses with their copy of the December 2016-February 2017 *ACAMS Today* magazine.

Has your *ACAMS Today* accompanied you on a business trip, an adventure or vacation spot? If so, we would like to hear from you. To submit an image, go to ACAMSToday.org or email editor@acams.org. We will be featuring these images in subsequent issues of the *ACAMS Today* and on Twitter @acamstoday.



▲ Vasu Sanghani, CAMS, assistant vice president, Bank of the West

▲ Todd Beck, CAMS, senior product manager, ACAMS

▲ HSI El Dorado Task Force

▲ Kaluwa Maitre-Avril, principal consultant, THRONE Compliance Services, Ltd.

Thephil Russelliah Roby, CAMS Riverwoods, IL, USA

Thephil Russelliah Roby has over 12 years' of experience with financial institutions in the creation and development of their anti-money laundering and sanctions programs, both in the U.S. and abroad. Currently, Roby serves as director for Enterprise AML Governance and Risk at Discover Financial Services in Riverwoods, Illinois. In this capacity, Roby designed and launched the enterprise AML function in order to provide enhanced governance and oversight through the development of consistent standards and practices throughout the organization. Under her leadership, enterprise AML has established, among other things, a holistic enterprise-wide risk program (for risk assessments, country risk, monitoring for new risks/threats, etc.), a policy/procedure framework, a comprehensive training program and an ongoing monitoring and testing program for key controls. In addition, Roby created and launched Discover's Enterprise Sanctions and List Screening function, allowing for improved governance, consolidated investigations and enhanced technology capabilities for enterprise-wide acquisition, portfolio and transactional screening.

Prior to joining Discover, Roby held several leadership positions at BMO Financial Group, including serving as director and head of AML—Europe in London, U.K. In this role, she successfully led the design and execution of a comprehensive AML and sanctions program for the scope of the European business and oversaw integration activities of a key acquisition.

Furthermore, Roby has a master's in leadership and change management from DePaul University in Chicago, with distinction, and received her CAMS certification in 2007.

Marios M. Skandalis, FCCA, CFC, CFE, FICA, Nicosia, Cyprus

Marios Skandalis is a fellow member of the Association of Chartered Certified Accountants (U.K.), a licensed member of the Association of Certified Fraud Examiners (U.S.) and a Certified Financial Consultant.

In addition, he is a fellow member of the International Compliance Association (U.K.), a member of the Society of Corporate Compliance and Ethics (U.S.) and a member of the Association of Certified Anti-Money Laundering Specialists (ACAMS).

Today he is the director of the Group Compliance Division of the Bank of Cyprus Group. In this role, he successfully led the demanding compliance and anti-financial crime enhancement program over the last three years leading to the cultural transformation of the bank, setting it as a benchmark and a model financial institution in Europe. To this respect, Bank of Cyprus was awarded the *2017 Best Corporate Governance Corporation in Cyprus Award* by World Finance (U.K.), the *2016 Award for Best Transparency and Anti-Corruption Practices* by Transparency International Cyprus and the *2017 Award for Best Bank in Cyprus* by Corporate Insider (U.K.).

His professional career commenced in 1995 when he served as an audit supervisor and a senior management consultant with Ernst & Young in the Southeastern European region. In 2000, he moved to the Bank of Cyprus Group and took the post of chief financial officer of the General Insurance of Cyprus for over a decade. He then took the post of manager for the Organization of the Bank's Overseas Operations until 2013 when he was appointed as legal representative and head of the Bank of Cyprus' operations in Greece.

Sven Stumbauer, CAMS New York, NY, USA

Sven Stumbauer is the managing director at AlixPartners. In this role he leads AlixPartners' global anti-money laundering (AML) and sanctions practice, serving clients across North America and Latin America, the Caribbean, Europe and Asia. Stumbauer's industry expertise includes U.S. and international financial institutions, regulatory compliance, fraud issues, AML and Office of Foreign Assets Control (OFAC) compliance.

He has a wealth of experience leading complex, high-profile cross-border projects, providing assistance to clients and regulatory bodies in over 40 countries. In particular, he has led major engagements involving AML/OFAC compliance, fraud and corruption investigations, transactional due diligence and compliance training to both financial institutions and regulators throughout the world. Stumbauer has also provided expert guidance to leading financial institutions and their boards of directors on compliance with AML, OFAC regulations, and the Foreign Corrupt Practices Act.

In addition, Stumbauer has hands-on experience providing advisory services around government matters involving Deferred Prosecution Agreements, Cease and Desist Orders and Memorandums of Understanding. He has led numerous matters and/or provided reports to various governmental agencies, such as the U.S. Department of Justice, the Securities and Exchange Commission, the Financial Industry Regulatory Authority, the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the New York Department of Financial Services and foreign government agencies.

We may never pass this way again—So fortunate to be in AML!

The money laundering challenge in the U.S. and globally is a relatively recent issue. Starting with the drug trafficking crisis in the 1980s, the U.S. passed the first laws covering the movement of illicit funds in 1986 and the now well-known Financial Action Task Force (FATF) organized in 1989 to create an international response to the ever-growing problems associated with money laundering. I have been honored to have been a part of both the struggles and successes of what is now the anti-money laundering (AML) community throughout these 30 plus years. We have much work to do, but no one can deny that law enforcement, the broad financial sector and the supervisory agencies have all been committed to protecting society from those who prey on victims through the misuse of monies or items of value.

Our mission needs to be collaboration, communication and cooperation in this essential endeavor. I have tried to follow this mantra since I entered AML and will continue this strategy as I leave ACAMS as the executive vice president immediately after our annual conference in Las Vegas.

With the growth of ACAMS to over 50,000 members and closing in on 65 to 70 chapters worldwide, it is a good time for me to pursue other endeavors while still working closely with ACAMS on the advisory board, conference task forces and occasional columns for this great publication. AML in 2017 needs advocates for financial inclusion, to combat human trafficking and to offer recommendations on how to improve the compliance infrastructure—all issues I am committed to working on to seek solutions.

Having been on the inaugural ACAMS advisory board in 2002 and serving as chairman prior to joining the staff in 2010, I have always been so impressed by our members and their desire to share information, learn from each other and assist anyone that seeks their guidance. We truly are a community and that makes me proud.

Dedication and commitment

AML in 2017 is vastly different than in 2002, not to mention 1986 when the first AML laws and regulations were created. To be effective today in our profession demands an understanding of a vast array of financial products, crimes far beyond drug trafficking, and how to utilize technology to manage the risks inherent in using the financial sector. Record keeping and reporting is no longer enough. Successful AML requires risk assessment, advanced training and ensuring enough information and awareness by boards and senior management to have a strong "tone at the top." We have kept these goals in mind at ACAMS, but we rely on our members to make sure we produce tools to assist you in your endeavors, so keep us honest going forward. I am confident that the staff will continue to serve the membership so that you are successful in your challenges.

A brief thank you!

As I transition to teach, write and continue my podcast *AML Now*, I will have many opportunities to thank key members in my career that have helped me in my attempts to improve the AML community. For now, I want to note a few individuals that have been great partners in our collective goals mentioned above. Rick Small, our advisory board chair and good friend for more years than we both care to admit, has been a sounding board, a mentor and committed AML leader who has done so much for our community. Dan Soto, our first chair, set the template for ACAMS and I have tried to follow that model. Dennis Lormel, a true patriot, has been and continues to be, committed to ensuring that our members have information on terrorist financing and acts as soon as they occur. We have all benefitted from his unwavering commitment to making sure AML includes all parts of the community—the essential private-public partnership which I share and try to live every day. William Langford—the young guy of the group—was so important in elevating human trafficking as an AML priority and making sure ACAMS kept this focus throughout my time here. William, it will continue I assure you.

There are others of course that have helped me with successes that I have had at ACAMS and I will continue to seek you out and thank you as well.

Finally, the growth and expansion of what we are today could not have happened without the great staff we have here at ACAMS. Our former CEO, Ted Weissberg, ensured we could bring together a strong team to address certification, publications, chapters, products and membership support. My partners were not only great to work with, but their dedication to you as members knows no bounds.

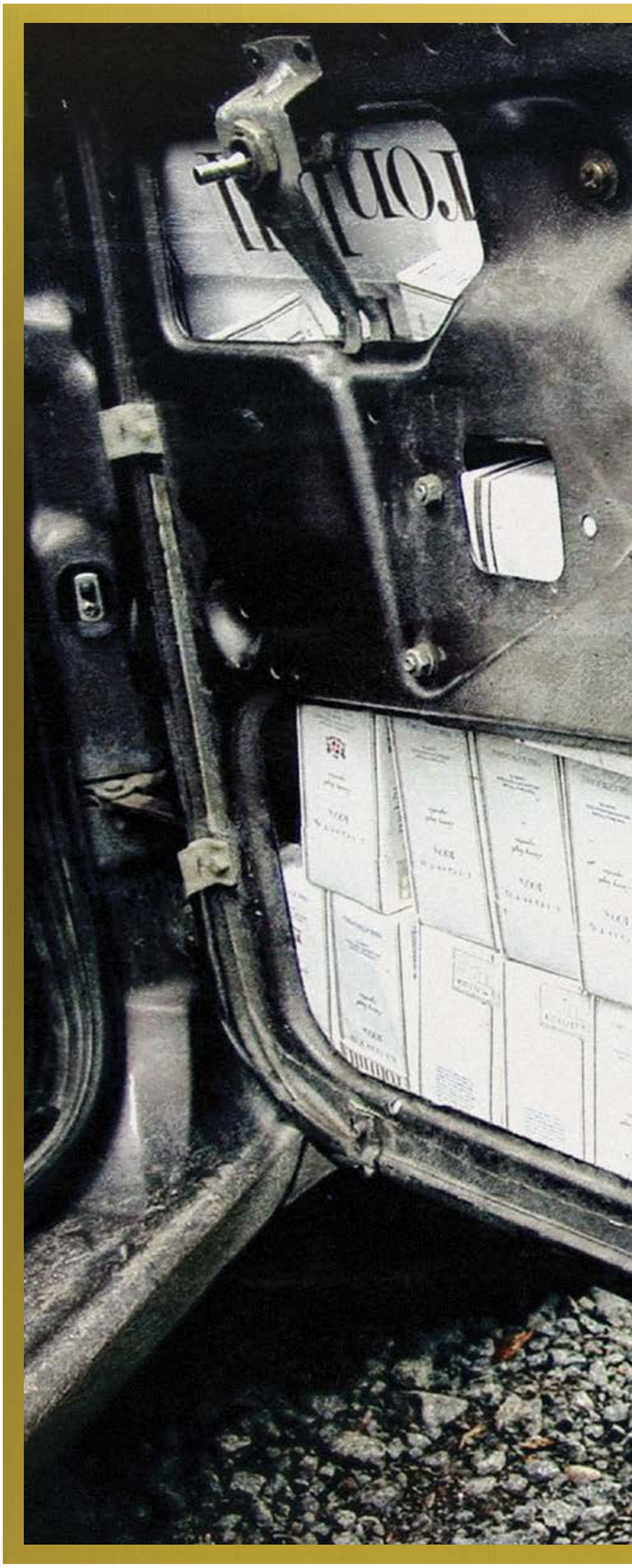
Thanks to all of you for the past 15 years of ACAMS and here is to many more! A

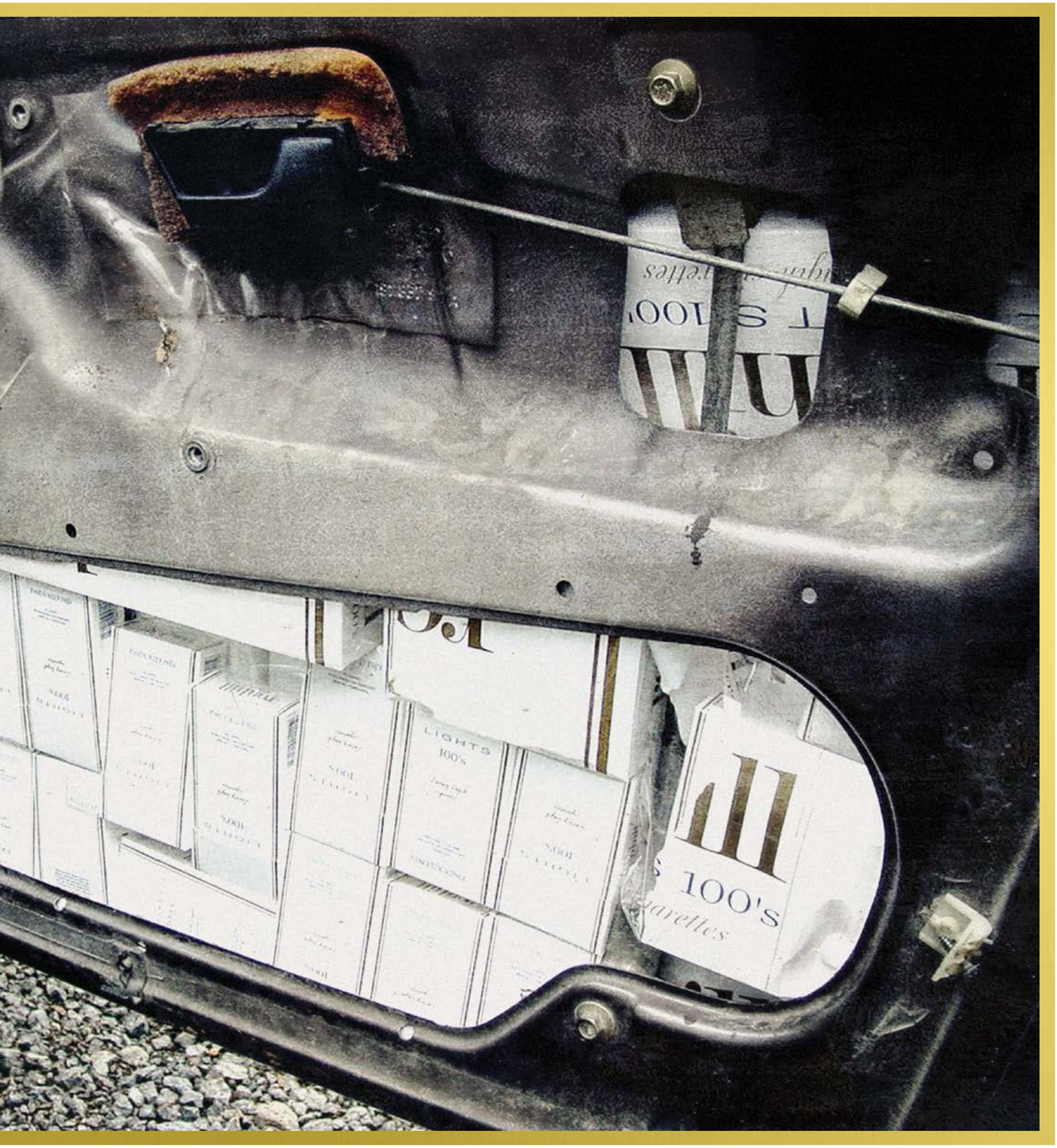
John J. Byrne, Esq., CAMS
executive vice president

Note: The title "We May Never Pass This Way Again" comes from Seals and Croft's 1973 album "Diamond Girl." My blog utilizes song titles and so I thought I would use that one more time in *ACAMS Today*. While we may never pass this particular way again, we will continue together in other ways.

EMERGING "MARKET" TRENDS

By now, certain shelf items have been labeled with a stock keeping unit (SKU), been advertised in circulars and placed out on display for resale. With the science of inventory management applied to market commodities for a quick profit, the question is should the abuse or misuse of these swiftly replenished items ever become a consideration factor for the financial institution's anti-money laundering (AML) monitoring? When are sales and product turnover "too good" and this deposited revenue indicative of the customer acting as a money laundering conduit? Could the financial industry be inadvertently misinterpreting a customer's profitability as a banner year instead of a surreptitious effort to sell to customers on the black and gray markets?




LIGHTS
100's
100's
S 100's
arettes

Demand forecasting is the art of predicting a customer's product desire. Businesses strive to foresee the future of commodities by implementing quantitative and qualitative assessments. Insight results in a drive in sales that leaves the market in the "black." However, the future of some goods is clear. Historical tax and import/export mandates, coupled with prevailing trends, all but assure the future of these highly profitable vendibles is so bright that retailers and financial institutions need to wear shades.

Authors have long documented the struggles associated with the sale of legal commodities, through a system of state and federal statutes and taxes, which become illegal upon transportation and/or misuse. Yet the supply and demand of various legal goods allow the retailer to deposit the proceeds, increase their account balances and continue to restock the items to perpetuate the profitable cycle and, by default (or in many cases intentionally), sustain black and gray markets. Alcohol, cigarettes, cellphones, syrup, cheese, and now various marijuana changing legalities are presently on the forefront of this topic. With each product, it was only when the introduction of man's greed for financial gain did the abuse commence of these otherwise legal commodities. Whereas, financial institutions documented the increased sales and/or purchases of exploited items as suspicious activity, the government also began to recognize the potential abuse of these commodities and their associated danger to the welfare of society.

As trafficked commodity proceeds were once placed directly into financial institution accounts, the trending presence of thriving money laundering conduits allows illicit monies to be exchanged at the retail level for exploitable items to only then be layered into the financial institution as "clean money." This pattern is reminiscent of a simplified, domestic Black Market Peso Exchange.

With the example of cigarettes, this legally sold tobacco product becomes egregious contraband once it crosses a state line. The ability to resell this product on the black market for a considerable profit margin, coupled with limited risk, is an invitation for high reward. Not only do the traffickers profit, but the wholesale businesses have an upsurge in bulk quantity sales. This black market commodity assures a high yield but also guarantees a growth in associated crimes. In fact, at a 2016 federal court sentencing of a cigarette trafficker, the presiding judge called cigarette trafficking "a clear and present danger to the health and welfare of the country."[1] Discount and convenience stores on highways near state borders all but advertise your last chance to be a cheat and avoid the higher fees and taxes found in your state. Literally, buses full of passengers make multiple stops to allow passengers an opportunity to purchase cigarettes in a "smurfing pattern" in an effort to circumvent reporting requirements, taxes and/or laws.

Communities are ravaged when contraband cigarette traffickers become targets of armed robberies, either for the tobacco product or for the cash used to purchase said commodities. The purchase of the cigarette cartons is typically conducted with currency in a structured format, in violation of federal law.

False businesses are often created to surreptitiously purchase the cigarette cartons and hide the true identities of the perpetrators. While some culprits have been identified, many wholesalers who sell the very commodity known to associate with funding terrorism, go largely undetected as the "money cleansing process" begins inside the store walls.

With the example of cellphones, phone trafficking "is driven largely by the massive profits made by exploiting the price difference between smartphones sold in the U.S. and overseas. Americans who agree to two-year service contracts with their cellphone company can buy the latest iPhones for about $200—a price subsidized by the carrier. In Hong Kong, an iPhone can be sold for as much as $2,000."[2] While some carriers have since nixed contracts and no longer subsidize the cost of the phone, the retail price for a cellular phone in the U.S. remains significantly cheaper than the expensive, international counterpart. This causes cellphone wholesalers, much like cigarette wholesalers, to rejoice over the net profits related to cellphone sales, and to happily peddle this commodity directly or indirectly overseas, contrary to law and export regulations.

[1] Frank Green, "Cigarette trafficker sentenced in federal court in Richmond to 16 months," *Richmond Times-Dispatch*, December 1, 2016,http://www.richmond.com/news/local/chesterfield/article_73b9da96-dd52-5b66-b84e-5b7683c53433.html

[2] Gerry Smith, "Inside The Massive Global Black Market For Smartphones," *Huffington Post*, July 22, 2013, http://www.huffingtonpost.com/2013/07/13/smartphone-black-market_n_3510341.html

RECOGNIZING THE POTENTIAL FOR FUTURE ABUSE ABATES WILLFUL BLINDNESS AND FINANCIAL INSTITUTIONS SHOULD BE COGNIZANT WHEN ANY COMMODITY SALE "LEAVES NORMAL" AND IS DEEMED "SUSPICIOUS"

Editorial Credit: Monticello/Shutterstock.com

As these particular commodities grew public notoriety, both traditional and non-traditional financial institutions followed suit and promptly documented the sale of this subject to abuse commodity and its identified red flag indicators. Furthermore, on several occasions they inadvertently identified the money laundering conduits responsible for furthering the criminal activity.

While retailers and wholesalers cannot control the intent of the customer, the very skill necessary to know what desired inventory to restock and henceforth preserve profitability, is the same talent that can be, but may not be, monitored by financial institutions. AML monitoring software is designed to detect an upsurge in anomalies. However, when are commodities properly identified as suspicious irregularities instead of being branded as a lucrative business profile because it is a yet-to-be identified trend? AML investigators have an opportunity to conduct their own version of forecasting by analyzing whether a drastic increase in sales and/or restocking purchases by their customer is indicative of a fad, a conventional commodity, or a money laundering conduit's trend worthy of being deemed a highly suspicious activity. Financial institutions have the ability to distinguish a high demand for a product by comparing and contrasting the known "norms" and cross-referencing the information with the know your customer (KYC) documents on file. The comparison of business profiles of like competitors in the same geographical area, can help scrutinize customers that sell commodities that can be easily flipped on the black and gray markets. Once again, highlighting the need for thorough and complete KYC documentation.

Financial institutions already have monitoring systems that identify the red flags associated with the identification of a high-risk product inventory; however, failure to recognize the propensity for a commodity's abuse upon resale and its known associated indicators is a concern. Recognizing the potential for future abuse abates willful blindness and financial institutions should be cognizant when any commodity sale "leaves normal" and is deemed "suspicious."

Moreover, detection and documentation of anomalies associated with vulnerable commodities by financial institutions would aid law enforcement in the fight against product exploitation. The identification of yet-to-be recognized items that can be resold on the black market and in turn put markets in the "black" is the crucial forethought necessary to combat money laundering and the underlying suspected unlawful activity by both traffickers and money laundering conduits. Lax and benign oversight is a mentality that (much like the black market commodities) has an expiration date. Who knew years ago that cheese would become "contraband dairy" and be the legal commodity behind major smuggling rings into Canada? Are sugary beverage tax hikes in Philadelphia now causing an upsurge in sodas sales outside of the region with certain distributors? Even more reason why analysis of legitimate products and the subsequent customer's profits should not be discounted.

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

WHO KNEW YEARS AGO THAT CHEESE WOULD BECOME "CONTRABAND DAIRY" AND BE THE LEGAL COMMODITY BEHIND MAJOR SMUGGLING RINGS INTO CANADA?

CYBERSECURITY:

NATION-STATE ACTORS, ENCRYPTED CYBERCRIMES AND MAN-IN-THE-MIDDLE ATTACKS

The harddisks of your computer have been encrypted with an military grad
encryption algorithm. There is no way to restore your data without a spe
key. You can purchase this key on the darknet page shown in step 2.
To purchase your restore your data, please fo
steps:
1. Download the Tor Browser at "https://www.torproject.org/". If
help, please access onion page".
2. Visit one of the ing pages with the Tor Browser:
http://golde onion/
http://golde .onion/
nter your personal decryption code there:
urchased your key, please enter it below.
for m1 = 1,M do begin
m2 = 1,M do begin
r u1 = u_min,u_max do begin
for u2 = u_min,u_max do begin
if u1 gt u2 then begin
for v1 = v_min,v_max do begin
if v1 lt u1 then begin
for v2 = v_min,v_max do begin
if v2 ge v1 then begin
KE_B = double(m1*u1^2+m2*u2^2)
KE_A =
endif
endfor

Illustrations by: Victoria Racine

CNN recently reported that the banking industry generally escaped the devastating impact of the global WannaCry ransomware attack.[1] Evidence is mounting steadily that North Korea was linked to this cyberattack and blame has also been directed at other countries.[2]

This article sheds light on the perplexing issue of cyberattacks by nation-state actors, given its diverse mix of stakeholders, disinformation, political and financial motivations, tools and methods deployed. In addition, this article explores two other cybersecurity concerns that impact financial transactions: encrypted cybercrimes and man-in-the-middle attacks.

Nation-state actors

Discussions of financial system vulnerabilities have been broadened to include warnings of cyberattacks by nation-states and their proxies.[3]

BankInfoSecurity[4] and *CNN*[5] recently reported on evidence that North Korea-linked hackers—a group referred to as Lazarus or Bluenoroff—have been behind recent cyberattacks on financial institutions in Africa, Asia, Europe, the Middle East and Latin America. Funds stolen through these cyberattacks have allegedly advanced North Korean nuclear weapons development.

International concern about nation-state sponsored cyberattacks on banks and other critical infrastructure date back at least 10 years.[6]

In 2007, Estonian authorities alleged that computer hackers, aligned with the Russian government, launched distributed denial-of-service (DDoS) attacks against Estonian banks and government agencies. These cyberattacks were reportedly a Russian response to an Estonian decision to move a Soviet World War II memorial from downtown Tallinn, leading to protests from the Russian government and ethnic Russians in Estonia. The Russian government denied involvement.[7]

In 2008, Georgian banks, government agencies and infrastructure were the targets of similar DDoS attacks, reportedly executed by computer hackers aligned with the Russian government. These cyberattacks coincided with Russian military action to curb Georgian efforts to increase its control over the South Ossetia and Abkhazia regions, which have had historically strong ties to Russia. The Russian government denied involvement.[8]

Fast forward to 2015, when U.S.- and U.K.-based banks topped the list of the world's largest and most interconnected global banks, as if to foreshadow cyberattacks targeting larger financial institutions that could have broader global consequences.[9]

In 2016, cyberattacks aligned with North Korea were in the news. Specifically, the North Korean government was suspected of launching cyberattacks against Asian banks in South Korea, the Philippines, Vietnam and Bangladesh for financial gain.[10]

In addition, in 2016, the U.S. Justice Department charged seven computer specialists, who reportedly performed work on behalf of the Iranian government, with cyberattacking U.S. financial institutions, such as Bank of America, NASDAQ, the New York Stock Exchange, Capital One Bank, ING Bank, Branch Banking and Trust Company, Fidelity National Information Services, U.S. Bank and PNC Bank.[11]

[1] Mark Thompson and Jethro Mullen, "World's biggest cyberattack sends countries into 'disaster recovery mode,'" *CNN*, May 14, 2017, http://money.cnn.com/2017/05/14/technology/ransomware-attack-threat-escalating/

[2] David Josef Volodzko, "Is North Korea Behind WannaCry Virus?," *South China Morning Post*, May 20, 2017, http://www.scmp.com/week-asia/geopolitics/article/2094980/north-korea-behind-wannacry-virus

[3] Gary Robbins, "Waging war with no bombs or missiles," *San Diego Union-Tribune*, October 28, 2016, http://www.sandiegouniontribune.com/news/science/sd-me-cyber-warfare-20161014-htmlstory.html

[4] Jeremy Kirk, "Kaspersky Links North Korean IP Address to Lazarus," *BankInfoSecurity*, April 4, 2017, http://www.bankinfosecurity.com/kaspersky-links-north-korean-ip-address-to-lazarus-a-9810

[5] Jose Pagliery, "North Korea-linked hackers are attacking banks worldwide," *CNN*, April 4, 2017, http://www.cnn.com/2017/04/03/world/north-korea-hackers-banks/

[6] Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News*, December 18, 2016, http://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111

[7] Associated Press, "A look at Estonia´s cyberattack in 2007," *NBC News*, 2009, http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/

[8] Jeremy Kirk, "Georgia cyberattacks linked to Russian organized crime," *Computerworld*, August 17, 2009, http://www.computerworld.com/article/2527019/government-it/georgia-cyberattacks-linked-to-russian-organized-crime.html

[9] Paul Glasserman and Bert Loudis, "A Comparison of U.S. and International Global Systemically Important Banks," *United States Treasury Department, Office of Financial Research (OFR) Brief Series* 15-07, August 4, 2015, https://www.financialresearch.gov/briefs/files/OFRbr-2015-07_A-Comparison-of-US-and-International-Global-Systemically-Important-Banks.pdf

[10] Nicole Perlroth and Michael Corkery, "North Korea Linked to Digital Attacks on Global Banks," *New York Times*, May 26, 2016, https://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html

[11] "United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi and Sadegh Ahmadzadegan a/k/a 'Nitr0jen26,' Omid Ghaffarinia a/k/a ´PLuS,´ Sina Keissar, and Nader Saedi a/k/a ´Turk Server," Sealed Indictment 16 CRIM 48, United States District Court Southern District of New York, https://www.justice.gov/usao-sdny/file/835061/download

Cyberattacks by nation-state actors, unscrupulous business competitors and their proxies may target not only personally identifiable information, but also corporate intellectual property, competitive trade secrets and confidential business information.[12]

Encrypted cybercrimes

Encryption is the conversion of data into another form or code, so that it might be read only by those who have access to a secret decryption key or password. Ciphertext refers to encrypted data. Plaintext refers to unencrypted or decrypted data.[13]

Warnings of cyberattacks by nation-states and their proxies have led information security leaders to support stronger encryption, so that data and financial transactions might be protected from malware and malicious third-party eavesdropping. In addition, cybersecurity leaders have opposed requirements for backdoors that could weaken encryption.[14]

However, stronger encryption can make financial crimes investigations more complex, as criminal organizations and terrorists take advantage of encrypted communications to evade detection.

North Korea has been linked to recent ransomware cyberattacks, in which hackers demand that victims pay a Bitcoin ransom for a decryption code to unlock data encrypted by a virus that infected the victim's computer or smartphone.[15] Evidence is mounting steadily that recent WannaCry ransomware attacks were orchestrated by North Korean hackers who operate in other countries.[16] North Korean representatives at the U.N. have denied links to the global WannaCry ransomware cyberattack. They have also denied the recent cyber hacking of a U.N. expert, who monitors violations of sanctions that are designed to prevent North Korean weapons development.[17]

To gain access to global banks and financial services, North Korea has reportedly evaded sanctions imposed by the U.N.[18] and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC),[19] by channeling transactions through agents and front companies operating outside of North Korea. North Korea also restarted its Cold War-era practice of using shortwave radio to broadcast encrypted messages, which may be directed at its spies or agents operating outside of North Korea.[20]

Latin American drug cartels have reportedly laundered money and created investigative blind spots by using encrypted networks[21] and apps to shield their electronic communications from surveillance.[22]

The Islamic State of Iraq and Syria (ISIS) has reportedly shielded its online communications from detection by using free TrueCrypt encryption software, which has been one of the strongest encryption programs since its release in 2004.[23]

In 2016, the *Miami Herald* reported the arrest of three members of Hezbollah, the Middle Eastern terrorist group that was suspected of laundering cocaine money for a Colombian cartel. The suspects reportedly used a complex global web of encrypted communications and financial transactions to move $500,000 into banks in Miami.[24]

[12] Steve Bychowski, "Cybersecurity 2017–The Year In Preview: Trade Secret Theft Takes Center Stage," *Security, Privacy and The Law*, November 21, 2016, http://www.securityprivacyandthelaw.com/2016/11/cybersecurity-2017-the-year-in-preview-trade-secret-theft-takes-center-stage/

[13] Nate Lord, "What Is Data Encryption?," *Digital Guardian*, January 27, 2017, https://digitalguardian.com/blog/what-data-encryption

[14] Robert Ackerman Jr., "The Rise of Nation-State Cyber Attacks Makes Encryption More Crucial Than Ever," *RSA Conference*, September 20, 2016, https://www.rsaconference.com/blogs/the-rise-of-nation-state-cyber-attacks-makes-encryption-more-crucial-than-ever#sthash.QHab4cq4.dpuf

[15] Paul Mozur and Choe Sang-Hun, "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*, March 25, 2017, https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html

[16] Choe Sang-Hun, Paul Mozur, Nicole Perlroth and David E. Sangermay, "Focus Turns to North Korea Sleeper Cells as Possible Culprits in Cyberattack," *New York Times*, May 16, 2017, https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper-cells-ransomware.html?_r=0

[17] Michelle Nichols, "North Korea says linking cyber attacks to Pyongyang is 'ridiculous,'" *Reuters*, May 19, 2017, http://www.reuters.com/article/us-cyber-attack-northkorea-idUSKCN18F1X3

[18] "Report of the Panel of Experts established pursuant to resolution 1874 (2009) - S/2017/150," United Nations Security Council, February 27, 2017, http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150&Submit=Search&Lang=E

[19] "Treasury Imposes Sanctions on Supporters of North Korea's Weapons of Mass Destruction Proliferation," *United States Department of the Treasury*, September 26, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl5059.aspx

[20] Choe Sang-Hun, "North Korea Revives Coded Spy Broadcasts After 16-Year Silence," *New York Times*, July 21, 2016, https://www.nytimes.com/2016/07/22/world/asia/north-korea-spy-radio-broadcasts.html?_r=0

[21] Alan Feuer and William K. Rashbaumjan, "U.S. Prosecutors Outline Case Against Mexican Drug Lord El Chapo," *New York Times*, January 20, 2017, https://www.nytimes.com/2017/01/20/nyregion/el-chapo-guzman-mexican-us.html?_r=0

[22] Patrick Howell O´Neill, "How a drug cartel used encryption and a fake website to launder millions," *The Daily Dot*, October 17, 2016, http://www.dailydot.com/layer8/mexican-cartel-encryption/

[23] Evan Ratliff, "The Strange Origins of TrueCrypt, ISIS's Favored Encryption," *The New Yorker*, March 30, 2016, http://www.newyorker.com/news/news-desk/the-strange-origins-of-truecrypt-isiss-favored-encryption-tool

[24] David Ovalle, "State: Hezbollah-linked group laundered drug money through Miami banks," *Miami Herald*, October 11, 2016, http://www.miamiherald.com/news/local/crime/article107366182.html

Encrypted communications and financial transactions may still be subject to legally compelled production and criminal investigations.[25]

Man-in-the-middle attacks

The European Banking Authority recently called for stronger encryption to secure communications for payment services and to prevent both manipulation by, and misdirection of communications to, unauthorized parties through man-in-the-middle attacks.[26]

In a man-in-the-middle attack, a cyber-attacker intercepts a user's online communications. Through this interception, the cyber-attacker might gather information as it is transmitted over the network. Computer and handheld device users are vulnerable to such attacks. Encryption can provide an effective safeguard against man-in-the-middle attacks.[27]

International cybercriminal groups have used man-in-the-middle attacks to intercept corporate payment requests, with the ultimate goal of having payments made into accounts that they control.

One such cybercriminal group included 49 suspects in Belgium, Cameroon, Georgia, Italy, Nigeria, Poland, Spain and the U.K. The 49 suspects allegedly used man-in-the-middle attacks to divert international fraudulent payments totaling 6 million euros over a relatively short period of time. European law enforcement made this investigation public following arrests of the 49 suspects, searches of 58 properties and seizures that included computers, disks, telephones, handheld devices, credit cards, SIM cards, memory sticks, forged documents and bank account documents.[28]

The FBI has warned of internet scams that similarly involve financial losses from man-in-the-middle attacks, including the email-related international Business Email Compromise (B.E.C.) scheme and Operation Romeo and Juliet, which involves victims who are targeted when they subscribe to online dating services.[29]

Vulnerable Wi-Fi hotspots expose personal and work devices to significant cyberattacks and financial losses. Yet, public awareness of this vulnerability is relatively low. Use of unsecure Wi-Fi hotspots can expose users to man-in-the-middle attacks that allow cybercriminals to invade personal privacy, including location-based tracking, message interception and conversation eavesdropping.[30]

Related cyberthreats include man-in-the-browser attacks, which can put online banking at risk. Man-in-the-browser attacks may allow a cyber-attacker to use a malware trojan to bypass encryption and intervene undetected in a legitimate authenticated online financial transaction. Such undetected intervention may allow the cyber-attacker to modify the

[25] Dan Terzian, “The Fifth Amendment, Encryption, and the Forgotten State Interest,” *UCLA Law Review*, 61 UCLA L. Rev. Disc. 298 (2014), http://www.uclalawreview.org/pdf/discourse/61-19.pdf

[26] “Final Report - Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2),” European Banking Authority, February 23, 2017, https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

[27] “Alert (TA15-120A) Securing End-to-End Communications,” United States Computer Emergency Readiness Team (US-CERT), United States Department of Homeland Security, September 29, 2016, https://www.us-cert.gov/ncas/alerts/TA15-120A

[28] Jeff Goldman, “Cybercriminals Use Man-in-the-Middle Attacks to Steal 6 Million Euros,” *eSecurity Planet*, June 12, 2015, http://www.esecurityplanet.com/hackers/cybercriminals-use-man-in-the-middle-attacks-to-steal-6-million-euros.html

[29] Vicki D. Anderson, “FBI Warns of Rise in Schemes Targeting Businesses and Online Fraud of Financial Officers and Individuals,” FBI, March 29, 2016, https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals

[30] Michael Covington, “Free Wi-Fi and the dangers of mobile Man-in-the-Middle attacks,” *betanews*, October 8, 2016, http://betanews.com/2016/10/08/free-wi-fi-mobile-Man-in-the-Middle-attacks/

JOIN THE CALL FOR STRONGER INTERNATIONAL AGREEMENTS AND ALLIANCES AMONG GOVERNMENTS AND LAW ENFORCEMENT AGENCIES

financial transaction as it occurs.[31] Other related cyberthreats include man-in-the-mobile, man-in-the-app, man-in-the-cloud and man-in-the-IoT attacks.[32]

In conclusion, on the perplexing issue of cyberattacks by nation-state actors, responses may include the following:

- Research cyberattacks by nation-state actors and commercial and governmental responses to such cyberattacks. Online search terms like "advanced persistent threats" (APTs) may be helpful. APTs often cover large-scale cyberattacks incited by nation-states—such as China, Russia, Iran and North Korea[33]—or by hacking groups, companies or organizations that serve as their proxies.[34] APTs may also include cyberattacks that are directed at major institutions by foreign terrorists and criminal organizations.[35]
- File timely suspicious activity reports (SARs), pursuant to the U.S. Department of the Treasury's Financial Crimes Enforcement Network's recently issued advisory to financial institutions on cyber-events and cyber-enabled crime.[36]
- In addition to filing SARs, other public-private information sharing options may include those outlined by the Cybersecurity Information Sharing Act of 2015 (CISA),[37] a U.S. federal law designed to encourage public-private information sharing on cyberthreats.[38] Please note:
  - — CISA is not a substitute for other federal reporting, such as timely SAR filings.[39]
  - — CISA submissions must be attentive to information privacy and cybersecurity concerns, given the possibility of a CISA data breach by cybercriminals, including nation-state actors and their proxies.[40]
  - — CISA has been criticized by information privacy and civil liberties groups, like the Electronic Frontier Foundation (EFF)[41] and the American Civil Liberties Union (ACLU).[42]
- Join the call for stronger international agreements and alliances among governments and law enforcement agencies, prompted by the recent wave of cyberattacks backed by nation-states.[43]

[31] Dauda Sule, "Man in the Browser—A Threat to Online Banking," *ISACA Journal*, Volume 4, 2016, https://www.isaca.org/Journal/archives/2013/Volume-4/Documents/13v4-Man-in-the-Browser.pdf

[32] Michael Gregg, "Six Ways You Could Become a Victim of Man-in-the-Middle (MiTM) Attacks This Holiday Season," *Huffington Post*, November 12, 2016, http://www.huffingtonpost.com/michael-gregg/six-ways-you-could-become_b_8545674.html

[33] Frank J. Cilluffo, "Emerging Cyber Threats to the United States," United States House of Representatives testimony, February 26, 2016, http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf

[34] Tom Spring, "Nation States Distance Themselves from APTs," *Threatpost*, February 14, 2017, https://threatpost.com/nation-states-distancing-themselves-from-apts/123711/

[35] Limor Kessem, "Organized Cybercrime's New Bull's-eye: Bankers," *SecurityIntelligence*, April 8, 2016, https://securityintelligence.com/organized-cybercrimes-new-bulls-eye-bankers/

[36] "FIN-2016-A005 Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," *United States Department of the Treasury - Financial Crimes Enforcement Network*, October 25, 2016, https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

[37] S. 754, "Cybersecurity Information Sharing Act of 2015," *Congress.gov*, October 27, 2015, https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf

[38] Brad S. Karp, "Federal Guidance on the Cybersecurity Information Sharing Act of 2015," Harvard Law School Forum on Corporate Governance and Financial Regulation, March 3, 2015, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

[39] "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015," United States Department of Homeland Security, United States Department of Justice, June 15, 2016, https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

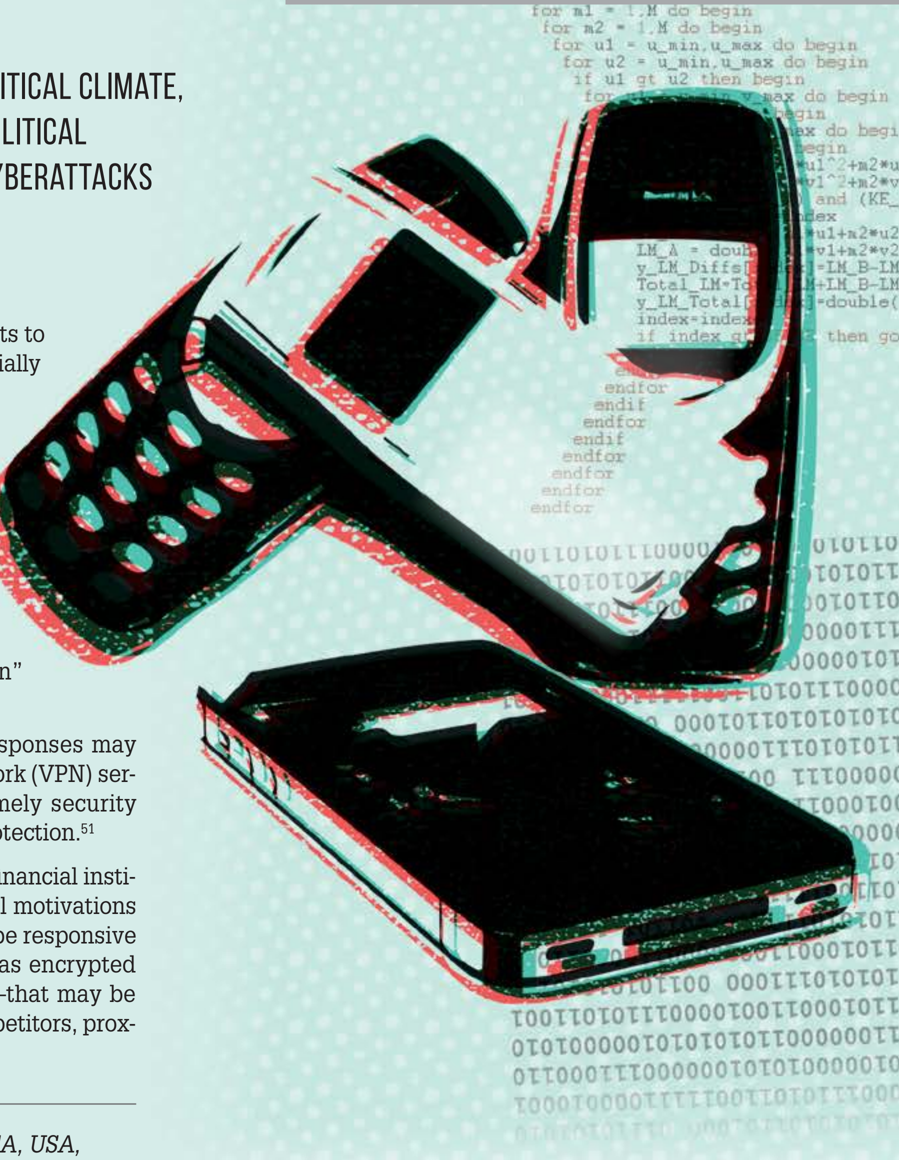
[40] Robyn Greene, "Is CISA gift-wrapped for hackers and nation-state actors?," *TheHill.com*, August 3, 2015, http://thehill.com/blogs/pundits-blog/technology/250070-is-cisa-gift-wrapped-for-hackers-and-nation-state-actors

[41] Lee Tien, "EFF Strongly Opposes CISA Cyber Surveillance Bill and CFAA Amendment," October 22, 2015, *Electronic Frontier Foundation*, https://www.eff.org/deeplinks/2015/10/eff-strongly-oppose-cisa-cyber-surveillance-bill-and-cfaa-amendment

[42] Eliza Sweren-Becker, "Congress Working in the Dark on Cybersecurity Bill," *ACLU.org*, November 17, 2015, https://www.aclu.org/blog/free-future/congress-working-dark-cybersecurity-bill

[43] Dustin Volz, "'Digital Geneva Convention' needed to deter nation-state hacking: Microsoft president," *Reuters*, February 14, 2017, http://www.reuters.com/article/us-microsoft-cyber-idUSKBN15T26V

TO SUCCEED IN TODAY'S GLOBAL BUSINESS AND POLITICAL CLIMATE, FINANCIAL INSTITUTIONS MUST BE ATTENTIVE TO POLITICAL AMBITIONS AND FINANCIAL MOTIVATIONS BEHIND CYBERATTACKS



Microsoft's president recently called on world governments to develop and adhere to global cybersecurity rules—essentially a modern-day "Digital Geneva Convention"—that would deter cyberattacks by nation-states.

On the encryption of cybercriminal communications and financial transactions, responses may include forced decryption,[44] subpoenas and search warrants,[45] detentions[46] and prosecutions,[47] although information privacy and civil liberties groups, like the EFF and the ACLU,[48] have raised significant objections. To look into ransomware related news and prevention tools, online search terms like "cyber extortion," "digital blackmail" and "cyber shakedown" may be helpful.[49]

On man-in-the-middle and man-in-the-browser attacks, responses may include cybersecurity solutions, such as virtual private network (VPN) services,[50] multi-factor authentication, digital signing and timely security updates to operating systems, applications and antivirus protection.[51]

To succeed in today's global business and political climate, financial institutions must be attentive to political ambitions and financial motivations behind cyberattacks. Cybersecurity risk management must be responsive to such evolving realities and to tools and methods—such as encrypted cybercrimes, ransomware and man-in-the-middle attacks—that may be deployed by nation-state actors, unscrupulous business competitors, proxies, drug cartels and terrorist groups.

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

[44] Dan Terzian, "Forced Decryption as a Foregone Conclusion," *California Law Review Circuit*, Vol. 6, May 2015, http://www.californialawreview.org/wp-content/uploads/2015/05/TERZIAN_27.pdf

[45] John M. Cauthen, "Executing Search Warrants in the Cloud," FBI, October 7, 2014, https://leb.fbi.gov/2014/october/executing-search-warrants-in-the-cloud

[46] David Kravets, "Man jailed 16 months, and counting, for refusing to decrypt hard drives," *Ars Technica*, February 12, 2017, https://arstechnica.com/tech-policy/2017/02/justice-naps-man-jailed-16-months-for-refusing-to-reveal-passwords/

[47] Orin Kerr, "The Fifth Amendment limits on forced decryption and applying the ´foregone conclusion´ doctrine," *Washington Post*, June 7, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine/?utm_term=.7462c3b87571

[48] "Brief of Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union in Support of Movant-Appellant and Reversal," United States Court of Appeals Third Circuit, No. 15-3537, April 6, 2016, https://cdn.arstechnica.net/wp-content/uploads/2016/04/effamicus.pdf

[49] Cheryl Tang, "Are All Ransom Attacks Considered Ransomware?," *Imperva.com*, June 22, 2017, https://www.imperva.com/blog/2017/06/are-all-ransom-attacks-considered-ransomware/

[50] Max Eddy, "The Best VPN Services of 2017," *PCMag*, July 19, 2017, http://www.pcmag.com/article2/0,2817,2403388,00.asp

[51] "Protecting Online Customers from Man-in-the-Browser and Man-in-the-Middle Attacks," *Arcot*, http://www3.ca.com/~/media/Files/whitepapers/protection-from-mitm-mitb-attacks-wp.pdf

Artfully done

Katsushika Hokusai (Japanese, Tokyo (Edo) 1760–1849)

The Metropolitan Museum of Art, H. O. Havemeyer Collection, Bequest of Mrs. H. O. Havemeyer, 1929

Under the Wave off Kanagawa (Kanagawa oki nami ura), also known as The Great Wave, from the series Thirty-Six Views of Mount Fuji (Fugaku sanjūrokkei) is one the most recognizable works of Japanese art in the world. This wood block print by the Japanese artist Hokusai, published between 1829 and 1833, embodies the beauty, movement and force of tidal waves on the lakes around Mount Fuji.

It seems a fitting illustration of the concepts of movement and change, which we are witnessing in 2017 when it comes to tackling financial crime.

The AML/CTF regulation tide

Concerned by the significant and evolving challenges of money laundering and terrorist financing, recent months have witnessed a series of recommendations and measures at international, European and national levels. It seems the tide of regulation is no longer confined to the financial sector with legislators extending their focus to new sectors of financial activity, including the art market.

For example, on June 26, 2017, the European Commission published a supranational risk assessment (SNRA) of money laundering and terrorist financing affecting the internal market.[1] The report identifies dealers in high-value goods and the art market as being sectors at risk due to what the report describes as their "inherent risk exposure and weak level of controls." It recommends member states extend their lists of obliged entities to include auction houses, art and antiques dealers and specific traders in high-value goods. On the same day, the U.K.'s new anti-money laundering (AML) regulations came into force.[2] Art businesses accepting cash payments above 10,000 euros in a single or series of linked operations are regulated as high-value dealers and in a change to the previous legislation are now required to register to carry out their activities.

When it comes to countering terrorism, the G20 published a new action plan on July 7, 2017. Amongst other measures, it calls on heads of state, governments and the private sector to dismantle connections between terrorism and transnational organized crime, including the looting and smuggling of antiquities. Within a week, the European Commission responded by publishing a proposal for a new regulation on the import of cultural goods.[3] The proposal is designed to close loopholes and to curb illicit trafficking suspected to be linked to terrorist financing activities.

This article looks at these issues and asks if further regulation is really the answer or if there are alternative and complementary methods of tackling financial crime.

Financial crime in the art market: A reality?

In November 2015, at a conference in Geneva organized by the University of Geneva's Art-Law Centre and the Geneva-based Art Law Foundation, representatives from the art market, Geneva Freeport, law enforcement and customs, as well as lawyers and academics came together to debate whether financial crime in the art market was a reality.

The absence of any reliable figures makes it practically impossible to gauge the extent to which money laundering may exist in the art market. With that said, the few high profile cases—which have come to light in recent years—demonstrate that the art market, like other financial markets, is at risk of abuse. In the layering stage of money laundering, criminals seek to separate the proceeds of their criminal activity from its illegal origin. Purchasing valuable assets such as artworks, artifacts or antiquities, helps to convert such "dirty" cash or funds into an asset that gains value and can be sold later.

Certain features of the art market (like other luxury goods such as real estate, yachts and cars), make it attractive to criminals seeking to launder the proceeds of crime or to finance illegal activities. These include:

- High-value goods
- International markets and networks
- Common use of intermediaries or proxies for transactions
- Common use of foreign/offshore structures and accounts
- Culture of discretion (the buyer and seller are often unknown to each other)

However, the art market also has features that can serve as a deterrent, including:

- Auction sales are public and highly publicized making them less attractive to criminals seeking to keep a low profile.
- Unlike cash or financial instruments, artworks tend to be unique, making them more easily identifiable and traceable.

[1] "Report from the Commission to the European Parliament and the Council on the Assessment of Risks of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities," European Commission,

[2] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, http://www.legislation.gov.uk/uksi/2017/692/made

[3] ”Security Union: Cracking Down on the Illegal Import of Cultural Goods Used to Finance Terrorism," European Commission, July 13, 2017, http://europa.eu/rapid/press-release_IP-17-1932_en.htm

- Art values fluctuate and this value volatility can make art less attractive as a means of placement or layering for money launderers.

Challenges faced by art businesses

Globalized and complex, the art market is constantly evolving. Art is increasingly being sold online and collected for investment, as well as for its aesthetic, cultural or historical value.

Online sales and non-face to face transactions, present increased risk and are boosting demand for online identification tools. The advent of modern technology and the ease with which documents can be forged, requires art businesses to be ever more vigilant.

In addition, the legal and regulatory framework within which art businesses are required to operate, is becoming increasingly complex and fragmented.

When it comes to AML and counter-terrorist financing (CTF) measures, certain countries have imposed regulations on art dealers in an effort to continue protecting the market from abuse. However, there is little international harmonization. For example, in France, auction houses and art/antique dealers fall within the regulated sector whilst in the U.K. they only become regulated entities if they accept cash payments at or above 10,000 euros for a single or series of linked transactions. In Switzerland, the cash limit is higher, CHF$100,000 and above.

For art businesses who transact internationally, this patchwork of fragmented legislation presents significant challenges. Art businesses need to understand and comply with AML/CTF laws in a number of jurisdictions (e.g., the situation in the U.K. and France is different to that in Switzerland, the U.S., Asia and so on).

The response of the larger auction houses and industry players has been to invest in dedicated compliance teams to tackle these issues and manage the risk. However, this solution is not available to smaller art businesses, galleries and dealers who lack the financial and human resources to invest in such infrastructure.

Regulation versus self-regulation

The role and place of regulation and self-regulation in the art market has been a topic of hot debate.

Regulation

The European Commission, in its recent SNRA, advocates extending existing AML regulation to auction houses, art and antiques dealers and specific traders in high-value goods. In addition, it recommends a number of more practical measures including:

- Extending national risk assessments to include cultural artifacts and antiques;
- Carrying out sufficient unannounced spot checks on high-value dealers, especially gold and diamonds, to identify possible loopholes in compliance with customer due diligence requirements; and
- Promoting awareness raising campaigns among art dealers, encouraging them to apply AML/CTF measures.

In the same report, the Commission acknowledges that regulation alone does not necessarily result in better outcomes. For example, when discussing the identification of beneficial ownership information it questions whether the mechanical application of rules by certain obliged entities leads to the identification of the real beneficial owner.

Self-regulation

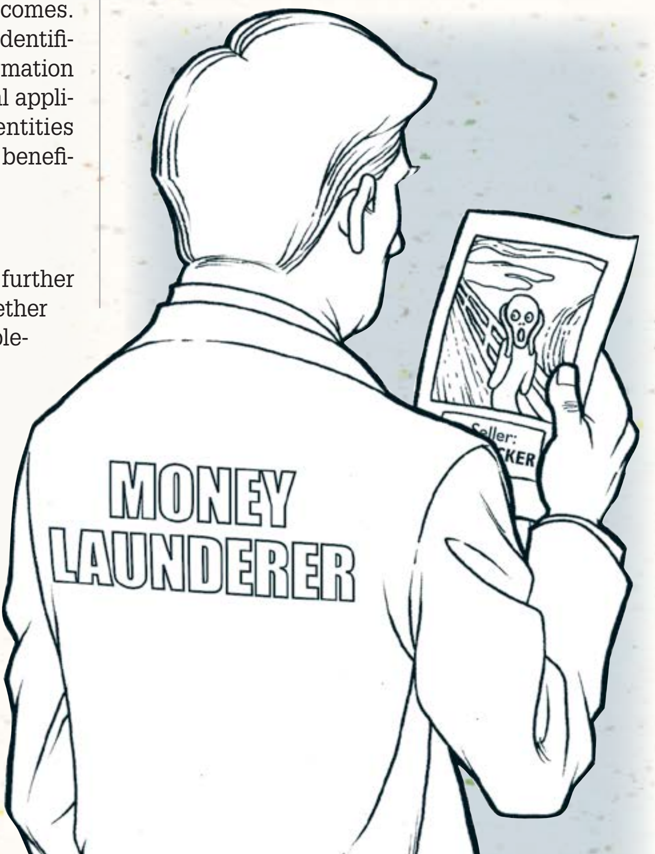
All this begs the question, whether further regulation is really required and whether a better approach would be to complement the existing legal framework with industry driven, self-regulatory codes of conduct.

Interestingly, U.S. economist Nouriel Roubini, who at the World Economic Forum warned that art was being used as a form of money laundering, went on to say that regulation was not necessarily the solution. In his words, "Self-regulation probably might be the right way to go for now."

Can self-regulation in the art market make a difference?

For a market as complex, diverse and constantly evolving as the art market, self-regulatory approaches are widely recognized as having several advantages over state-imposed regulation. These include:

- **Flexibility and speed** – Industry guidelines can be developed and updated more quickly than state-imposed legislation, which takes time to be approved and adopted. For example, the proposed new EU regulation on the import of cultural goods, if adopted, will take two years to be transposed into national legislation. However, self-regulatory measures can be updated more quickly to respond to evolving threats resulting in greater operating efficiencies for art businesses and in turn minimizing compliance costs.
- **Better adapted** – Greater technical and industry expertise can be achieved through industry developed guidelines, which strike that critical balance between achieving the desired goal whilst not stifling the market so much that it cannot operate.



- **Collaborative** – Conflicts of interest are mitigated through the participatory design process.
- **Global** – Unlike legislation, which is territorial, guidelines and codes of conduct can transcend national boundaries, resulting in a more flexible approach better adapted to serving a global market, such as the art market.

The Responsible Art Market Initiative

To contribute to the discussion on best practices and compliance in the art market, January 2017 saw the launch of the Responsible Art Market Initiative (RAM) together with its online platform.[4] This non-profit industry initiative was formed in Geneva in November 2015[5] under the auspices of the University of Geneva's Art-Law Centre and the Geneva-based Art Law Foundation and it is the first of its kind.

RAM exists to support art market actors providing them with a practical and ethical compass to navigate the increasingly complex and fragmented legal framework within which they are required to operate. It aims to do this by:

- Raising awareness amongst art market actors of risks which they face in conducting business;
- Consolidating and sharing existing industry best practices; and
- Doing so through practical guidelines and tools that can be easily understood and implemented.

Risk-based AML/CTF guidelines

RAM's first set of guidelines tackle the issue of money laundering and terrorist financing threats in the art market. They adopt a risk-based approach and emphasize the importance of art businesses knowing their clients and being alert to red flags.

The guidelines are supplemented with a quick reference guide, easy-to-use red flag lists and country guides providing an overview of the AML regimes applying in different jurisdictions.[6] RAM's red flag lists are tailored to art transactions and they focus on three areas of inquiry: the client, the artwork and the transaction itself.

Client red flags include:

- Agents acting for undisclosed buyers or sellers
- Offshore companies, trusts and foundations

Artwork red flags include:

- An artwork presented with limited or no documentation or provenance
- Sellers who refuse or are reluctant to provide written evidence of provenance
- An artwork, which is an antiquity or whose source country is or has been in recent conflict

Transaction red flags include:

> WHAT MAKES RAM UNIQUE IS ITS COLLABORATIVE, INTERDISCIPLINARY APPROACH

- Clients who knowingly wish to sell at an artificially low or inflated price
- Sellers who are unwilling or unable to provide adequate proof of ownership for items they wish to consign for sale
- Buyers who insist on making multiple low-value cash payments for a single or series of connected transactions

RAM sees its practical, self-regulatory approach as complementing existing state-imposed regulation. Its guidelines are designed to be accessible to the entire market, including small art businesses and individual dealers and collectors who do not have the financial resources to spend on large compliance departments or expensive lawyers.

A different approach

What makes RAM unique is its collaborative, interdisciplinary approach. RAM's founding members span the entire spectrum of the art market, from international auction houses (Christie's) and individual dealers (Seydoux & Associés) to services providers (the Geneva Freeport and SGS art services), specialist art lawyers and academics from the University of Geneva's Art-Law Centre and Geneva-based Art Law Foundation, as well as law enforcement.

This cross-industry participation ensures issues are addressed holistically from various perspectives. By cooperating to share and internalize existing best practices throughout the industry, RAM aims to have a greater impact when it comes to reducing risks for art businesses and collectors alike, thereby increasing public trust and confidence in the market.

Since launching, RAM has generated a positive response and global interest. It intends to build upon this, expanding its platform to address topics of specific concern to the art market with the constant goal of identifying and sharing responsible practices in the art market.

Conclusion

As the tide of regulation turns toward the art market, with the birth of initiatives such as RAM, perhaps it is time to transition to more collaborative and complementary methods of tackling financial crime.

For more information, visit http://www.responsibleartmarket.org. RAM will be holding its next annual conference in February 2018 in Geneva, Switzerland.

Mathilde Heaton, lawyer and art law consultant, Art Law Advisory, coordinator of the Responsible Art Market Initiative and researcher at the Art-Law Centre, University of Geneva, Geneva, Switzerland, mathilde@artlawadvisory.com

[4] http://www.responsibleartmarket.org

[5] RAM is the outcome of the November 13, 2015, conference organized by the University of Geneva's Art-Law Centre and the Geneva-based Art Law Foundation titled "Money Laundering in the Art Market: A reality?"

[6] All the materials are available for download from RAM's website: http://www.responsibleartmarket.org.

Casinos should bet big on enhanced AML surveillance

Anti-money laundering (AML) and financial crime as a whole, has been a growing concern within the gaming industry as casinos continue to navigate how best to control the flow of illicit funds through their gaming operations. Casinos are facing greater regulatory pressure to prevent money laundering and increasingly have been spending time and resources on enhancing their AML compliance programs in order to align with this heightened regulatory scrutiny.

Regulatory regimes around the world have been focusing more and more on casinos' obligations to develop effective systems for preventing and detecting money laundering. Many countries and jurisdictions have seemingly ever-expanding laws in place requiring financial institutions and casinos to assist in the fight against money laundering and other financial crimes. Macau recently updated its AML laws to impose regulations for junket operators and included more comprehensive internal control requirements for both casinos and junket operators. These enhanced requirements for casinos include identifying "bad actors" and potentially suspicious transactions and reporting these to the proper authorities. Similarly, the EU's Fourth AML Directive also expands requirements on both land-based and online casinos. Casinos are constantly challenged with balancing the need for operational transparency with law enforcement and the needs and discretion of their patrons. The increase in regulatory scrutiny is forcing casinos to rethink how they identify and monitor suspicious activity, and how to effectively enhance their AML compliance programs to mitigate these risks.

With greater scrutiny usually comes increased enforcement. The consequences for failing to implement robust AML, anti-bribery and corruption, and other financial crime-related controls can be quite staggering, and this trend is expected to continue. Recent enforcement actions have not only resulted in massive fines for gaming companies, but also consistently reveal the failures of casino operators to implement and maintain effective AML surveillance programs (i.e., identifying, investigating and reporting potentially suspicious levels of gaming activity). This regulatory pressure only amplifies the need for casinos to implement more holistic and automated AML transaction monitoring.

Responding to increased scrutiny

Continued regulatory actions and fines against casinos, card clubs and race/sports book operators alike, have driven the gaming industry to prioritize and invest in AML compliance by establishing risk-based compliance programs to prevent potential money laundering. Specifically, casinos have made efforts to improve the foundational elements of their AML compliance programs, including implementing comprehensive risk assessments, enhancing policies and procedures, investing in employee training and performing greater patron due diligence. The efforts to improve AML compliance in the gaming industry was also recognized by the Financial Action Task Force (FATF) during its 2016 mutual evaluation of the U.S.

FATF's report acknowledged the significant investment casinos have made to prevent money laundering, including an increased focus on raising awareness and improving AML compliance.

While casinos have made great strides in enhancing their AML compliance programs, there is still room for improvement. As money laundering continues to become more complex, the tools used to mitigate these risks must also evolve. Casinos can further enhance their compliance efforts by mining their data more effectively and incorporating automated tools to better monitor gaming activity for unusual or potentially suspicious levels of play. The use of data is most effective when it can be compiled and viewed across the entire organization, facilitating a single view of each patron and their corresponding activity.

While casinos have made great strides in enhancing their AML compliance programs, there is still room for improvement

Benefits of automation

By using an enterprise-wide technological solution, casinos are able to enhance their analysis of existing internal data, better monitor their patrons' activities, and automate processes, such as required regulatory filings. Doing so will enable casinos to focus on identifying and monitoring true risks.

Like other financial institutions, casino operators are increasingly using technology to better analyze the large amounts of collected patron data and leveraging this information in order to meet their know your customer (KYC), currency transaction reporting and suspicious activity reporting obligations.

Specifically, technology can be used to:

- Dynamically risk rate new and prospective patrons;
- Synthesize the results of sanctions and watchlist screening and adverse media searches;
- Drive a consistent application of KYC requirements by automatically prompting or triggering the appropriate level of patron due diligence measures to be conducted;
- Monitor transactional activity against known red flags (e.g., minimal play, chip walking, bill stuffing) or against baseline of expected activity within a particular peer group of players;
- Conduct and document investigations on alerted activity;
- Efficiently produce and file currency transaction reports (CTRs) and suspicious activity reports (SARs);
- Holistically view a patron's profile, including their gambling activity and relevant "AML history" (e.g., prior CTRs, SARs, date of last KYC review), across properties; and
- Proactively identify patterns of transactions, allowing for more robust due diligence reviews, better identification of discrepancies in patron activity, and more informed decision making.

Even more importantly, an enterprise-wide case management module can collect, aggregate and analyze patron data; thereby, allowing for consolidation of alerts and/or cases at the patron level, which leads to more comprehensive and productive investigations. In addition, a case management tool provides enhanced metrics and reporting capabilities to AML compliance departments, as well as a robust audit trail to evidence and support the conclusions reached on investigations.

Technology solutions can also provide a way for casinos to centrally manage their regulatory reporting. For instance, a technological solution can allow a casino to automatically generate requisite regulatory filings (e.g., SARs and CTRs) and management reports across the entire organization and facilitate the identification of joint filings, when appropriate. This enhances a casino's ability to share information at the enterprise level, as well as with regulatory authorities.

TECHNOLOGY CAN HELP CASINOS BETTER UNDERSTAND AND DEAL WITH THE RISKS PRESENT THROUGHOUT THEIR ORGANIZATION

Implementing an enterprise-wide technology-based solution

Over the past year, casinos have begun to realize the potential and importance of technology and analytics in combating money laundering and financial crimes. Implementing these types of solutions can help casinos produce more efficient AML reporting and better analyze and manage money laundering risk. However, challenges also exist when trying to implement an enterprise-wide solution. Automating manual processes not only exposes antiquated processes and business functions, but requires business teams to be more flexible, adaptable to change and available to receive additional training.

Gaming entities are often made up of separate properties that are different legal entities, each with its own gaming license from its applicable state gaming control board. Due to this structure, each property often has its own compliance function that has separate and distinct requirements, making consolidation, standardization and centralization of requirements challenging.

Implementing new technological solutions into existing systems often requires dedicated time and resources to deploy the solutions across the organization. For example, data mapping requests associated with new software implementations often expose missing, inconsistent and/or poor quality data, which require additional support to remediate. However, the amount of time and resources dedicated to a successful implementation is actually an investment that leads to a reduction in total resources in the long run.

Although implementing an enterprise-wide solution has it challenges, casinos can widely benefit from these technological advances.

Technology can help casinos better understand and deal with the risks present throughout their organization, allowing them to better monitor transactions, conduct more thorough investigations and produce accurate and timely regulatory reporting.

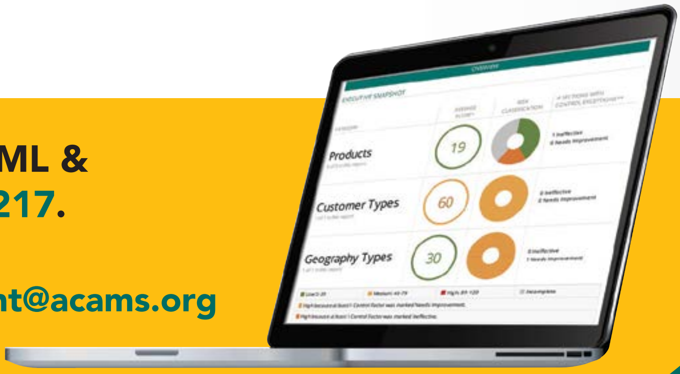
As regulators have continued to stress the importance of maintaining an effective AML compliance program, automation can help casinos continue to improve their efforts in mitigating money laundering and other financial crime risks.

Vasilios Chrisos, CAMS, ACAMS global advisory board member, principal—Financial Crimes Unit, PwC, New York, NY, USA, vasilios.p.chrisos@pwc.com

Contributing authors: Paul Havalchak, director, PwC, Las Vegas, NV, USA, paul.havalchack@pwc.com

Heather Finlay, manager, PwC, New York, NY, USA, heather.a.finlay@pwc.com

Allison Wadness, CAMS, manager, PwC, New York, NY, USA, allison.wadness@pwc.com


Products
19
Customer Types
60
Geography Types
30

YOU HAVE BEEN HIT WITH AN ENFORCEMENT ACTION— NOW WHAT?

An enforcement action is one of the most painful experiences in the life of any institution. Enforcement actions come in all types, shapes and sizes—in areas ranging from financial crimes compliance to consumer protection to trading room misconduct. They may be informal and private, or formal, public and enforceable in court. They can result in reputational damage, fines and penalties, along with labor-intensive remediation, monitor and independent consultant activities—all impacting the bottom line. These activities command the immediate attention of team members, diverting them from maintaining and growing the business.

In a worst-case scenario, credibility with your regulators is damaged, sometimes requiring a change in senior management and even in the board of directors. In cases where a monitor is assigned by regulators or law enforcement agencies, interacting with them will require even more time and attention than working with internal audit staff. Examinations of banks under a formal or even informal action can be intense, broad-based, multi-year and expensive. Got your attention?

Denial

If you have already made a mistake in the eyes of regulators or law enforcement, do not make another by going into denial over a looming enforcement action. Too many companies do this. It delays rallying the necessary resources and funds to effectively and efficiently remediate the cited issues. Compounding your errors by refusing to recognize reality is a major misstep. Complaining about the situation and arguing with examiners is often counterproductive, because over the long term, you have to work with your examiners. Put anger and frustration aside and take time to understand what the issues are, including root causes. As much as six months may elapse from the time examiners first advise you of their concerns and the issuance of an enforcement action. Do not waste this time—use it to get started on remediating the regulators' concerns. One of the most powerful things you can do is to let the regulators know that you get it and that you will take every action necessary to correct the problems.

Money

Once you are cited, an investment is required to remediate the issues, so you need to accept that fact. Not only will you have to spend money to address and correct problems identified in the enforcement action, but the institution, as well as individuals, may also face fines and restitution. Get a forecast together and reserve for the worst-case scenario. Make sure that you have the right people providing input. It cannot just be the finance department's job to get a handle on the costs. Do not forget to consider opportunity cost (the business you did not get and the loans you did not make because you were distracted or restricted by a compliance misstep). All stakeholders need to be consulted—from the business lines and executive leadership up to and including the board of directors. In addition, regularly refresh your budget.

People

Your institution probably lacks one or more of the appropriate staff, policies, procedures and tools for an effective program. This means that you will need to assess current staff, hire new staff in a highly competitive environment, and purchase and implement the automated tools necessary for your compliance program (e.g., anti-money laundering monitoring or Office of Foreign Assets Control sanctions administration). Not everything will go right either, particularly when you are dealing with data and systems. The board and senior management need to commit sufficient funds to strengthen a system of internal controls to ensure that it is appropriate to the risk profile of the institution. It is important that your institution be proactive in developing and executing a plan in a timely manner. Your monitor or independent consultant will guide you in this process through their independent reviews.

You will need staff who know the law and program elements and staff who know how to execute. Unfortunately, not everyone has every attribute. In fact, more often than not you will find that most staff have one or the other. Execution is key; it is also where most institutions fail. Make sure you have the right complement of people with these attributes.

Project management is extremely important. There will be many issues to be addressed with far-reaching remediation efforts throughout the company. A project management office needs to be established, surrounding the entire remediation effort. This will help to ensure that the wing-to-wing remediation efforts of the firm are fully documented with sustainable corrective actions and tracked through closure. In turn, this documentation will provide senior management, the board, regulators and law enforcement with a much higher degree of comfort that you know what you are doing and are on top of every aspect of your program enhancements.

COMPLIANCE DEPARTMENTS ARE VIEWED AS COST CENTERS WHEN THEY SHOULD BE VIEWED AS REVENUE GUARDIANS

Culture

The board and the CEO must be investing in, committing to, and actively communicating the change in company culture, with a renewed pledge to maintain an effective compliance program and to support the compliance department. The tone from the top must cascade down and around the entire company so that it resonates with every manager and employee. Everyone needs to understand that there is a new culture and that it is here to stay. Enforcement in a consistent manner is equally important. Employees and contractors need to know that violations will be dealt with swiftly and appropriately. Too often culture is overlooked, with institutions merely changing policies, procedures and processes. This approach is a proven misstep, since without a strong culture of compliance, your new policies and procedures may look good, but have little or no effect. There are actually methods to assess culture.

Do not repeat past mistakes

You finally get through the storm, wake up and the sun is shining. The enforcement action has been lifted. Your pulse is racing and you immediately start thinking about how you can cut costs. You begin rationalizing your staff and looking for further efficiencies. Time out. While it is generally a sound business practice to continuously seek efficiencies, do not fall into the trap of cutting costs or staff in a way that undoes all the work you have done to get your enforcement action lifted. You simply cannot go backward and expect that the same thing will not happen again.

Compliance departments are viewed as cost centers when they should be viewed as revenue guardians. Unless you have staff with the experience and tools to manage compliance, your institution is at risk of being sanctioned by any number of regulators and law enforcement agencies, to the detriment of your business. In the end, it is much less expensive to invest and get it right than to get it wrong. Thus, if you are hit with an enforcement action, it is important to recognize the following five points:

1. *Invest*—Enforcement actions will cost money. Recognize that the approvers of the remediation are the regulators and the monitors or independent consultants they appoint—not you.
2. *Think long-term*—There are no shortcuts. Sustainable programs take time and money.
3. *Partner and fix instead of opposing*—Partner with external and internal stakeholders, honestly assess where you are and move to the target state.
4. *Never let a crisis go to waste*—Use it to restructure and streamline your people, processes and systems.
5. *Hire the right expertise*—Cheap is expensive. Hire the right people with the right tools and experience.

Ross Marrazzo, managing director, Treliant Risk Advisors, New York, NY, USA, rmarrazzo@treliant.com

Bridging the gap between risk assessment and transaction monitoring

A robust money laundering/terrorist financing (ML/TF) risk assessment is the cornerstone of a sound compliance program. With more reliance on automated transaction monitoring systems, it is more important than ever to ensure that your transaction monitoring program is properly configured and aligned to the ML/TF risk profile of your institution.

On June 30, 2016, the New York Department of Financial Services (NYDFS) issued final rule part 504 requiring senior officers or board of directors to certify the effectiveness of anti-money laundering (AML) and Office of Foreign Assets Control (OFAC) transaction monitoring and filtering programs.[1] The final rule goes on to state that an institution's transaction monitoring program should be reasonably designed based on the risk assessment of the institution and appropriately matches BSA/AML/OFAC risks to the institution's businesses, products, services and customers/counterparties.

While conducting ML/TF risk assessments is not a new practice, it is the first time that ML/TF risk assessments are a written requirement for NYDFS-regulated institutions. This article will provide best practices for bridging identified ML/TF risks to your transaction monitoring program.

Identifying ML/TF risks within your institution

The board of directors and management set the risk appetite and are responsible for creating a culture of compliance to ensure staff adherence to the financial institution's compliance program. A robust risk assessment will help your financial institution to promptly and accurately identify risks and apply appropriate controls to mitigate risk or identify unacceptable risks to avoid. A sound risk assessment will identify potential events that might impact compliance objectives and should employ a combination of qualitative and quantitative risk assessment methodologies. The risk assessment should be utilized for the purpose of driving policy, procedures, controls and independent testing.

The risk assessment process has four main steps:

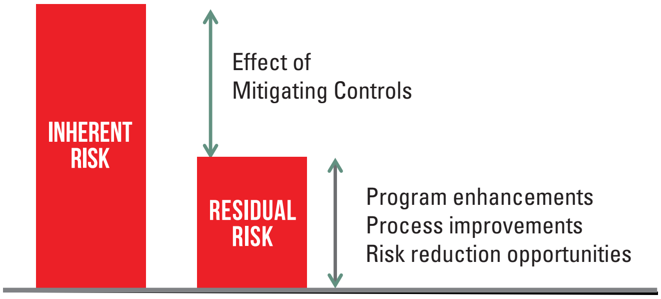
1. Identify the ML/TF inherent risks
2. Analyze the mitigating controls
3. Evaluate residual risk
4. Determine the direction of risk

Inherent risk is the risk that is present without regard to mitigating controls. Per the Federal Financial Institutions Examination Council's (FFIEC) BSA/AML Examination Manual,[2] a risk assessment should include an assessment of the financial institution's products, services, customers, entities, transactions and geographic locations. A sound risk assessment should include gathering relevant customer and transaction data and interviews of business line leaders. The composition of a complete customer and transaction database is the first step in understanding where the ML/TF risks are within your institution. It is best practice to include at least two years of customer and transaction data within your database as this helps identify potential trends utilized for determining the direction of risk.

[1] The final rule applies to banks that are chartered or licensed by New York, as well as nonbanks, such as money services businesses.

[2] FFIEC BSA/AML Examination Manual dated November 17, 2014, page 18.

THE COMPOSITION OF A COMPLETE CUSTOMER AND TRANSACTION DATABASE IS THE FIRST STEP IN UNDERSTANDING WHERE THE ML/TF RISKS ARE WITHIN YOUR INSTITUTION



The interview process is essential to obtaining a tailored and effective risk assessment and can assist with providing a qualitative assessment of the customer and transaction data. The interview process can identify ML/TF risks that were not previously identified and can help foster a line of communication between each business line and the compliance department. In addition, the interview process can help promote a culture of compliance by breaking down the silos of a traditional financial institution by encouraging information sharing and looking at ML/TF risks across the financial institution.

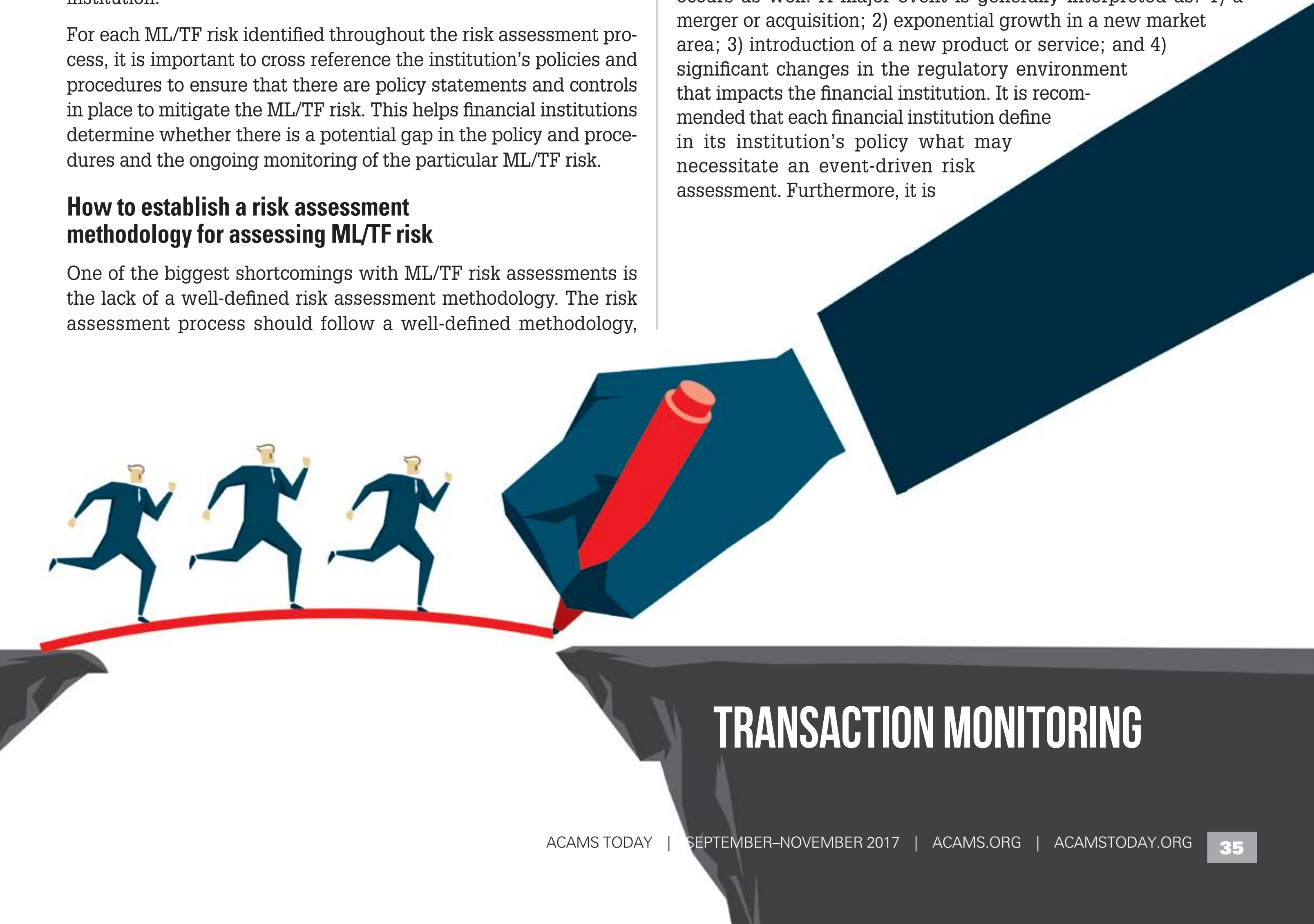
For each ML/TF risk identified throughout the risk assessment process, it is important to cross reference the institution's policies and procedures to ensure that there are policy statements and controls in place to mitigate the ML/TF risk. This helps financial institutions determine whether there is a potential gap in the policy and procedures and the ongoing monitoring of the particular ML/TF risk.

How to establish a risk assessment methodology for assessing ML/TF risk

One of the biggest shortcomings with ML/TF risk assessments is the lack of a well-defined risk assessment methodology. The risk assessment process should follow a well-defined methodology, which should be fully described in your risk assessment report and supporting documents. The risk assessment methodology should provide: 1) measurement of inherent risks accounting for the principals of impact and likelihood; 2) an assessment of the effectiveness of the mitigating controls; 3) an evaluation of the residual risks that exist after consideration of the mitigating controls; 4) a determination of the direction of risk for each risk; and 5) a process for determining the overall inherent and residual risk rating of the institution.

In addition, the risk assessment should incorporate new and emerging risks within the industry such as the FinCEN guidance FIN-2016-A005 on cyber-enabled crime and on how documenting cyber risk impacts a financial institution's ML/TF risk profile. It is important to remember that the risk assessment should be tailored for each institution and allow for the application of specialized knowledge/professional judgment by the compliance officer. The professional judgment factor can allow for an accurate reflection of the financial institution's risk profile based on intricate knowledge held by the compliance officer and/or stakeholders.

While risk assessments are typically conducted on an annual basis, it is often forgotten that it should be updated when a "major event" occurs as well. A major event is generally interpreted as: 1) a merger or acquisition; 2) exponential growth in a new market area; 3) introduction of a new product or service; and 4) significant changes in the regulatory environment that impacts the financial institution. It is recommended that each financial institution define in its institution's policy what may necessitate an event-driven risk assessment. Furthermore, it is



TRANSACTION MONITORING

important to note that a supplemental risk assessment and/or mini risk assessment can be completed in lieu of a full risk assessment when a major event occurs. Failure to have a well-defined methodology tailored to the financial institution that also incorporates recent trends and/or regulatory guidance can expose the financial institution to undue scrutiny from the independent auditors and/or regulators.

Aligning your ML/TF risk to your transaction monitoring program

Over the past 18 months, one of the most commonly cited areas of examiner AML criticism is the concept of sound model risk management and inadequate enterprise-wide risk assessments. Regulatory agencies have shifted resources and attention to assessing how institutions set up their automated transaction monitoring and high-risk customer management programs.

Financial institutions rely heavily on automated systems to identify potential suspicious activity but have been inundated with high levels of false positives, which have taken time and resources away from the ML/TF risks that require the most attention. Scenarios principally based on judgmental and quantitative considerations should be tailored to the institution's specific ML/TF risk profile.

A SOUND ENTERPRISE-WIDE RISK ASSESSMENT IS THE KEY TO BRIDGING THE GAP TO EFFECTIVELY IDENTIFY AND MONITOR ML/TF RISKS WITHIN YOUR FINANCIAL INSTITUTION

Conceptual soundness is the foundation for setting up an automated transaction monitoring model commensurate with your institution's ML/TF risk profile. Conceptual soundness involves assessing the quality of the model design and construction, as well as a review of documentation and empirical evidence supporting the methods used and variables selected for the model.[3] In setting up your transaction monitoring system, you should ensure that judgment exercised in model design and construction is well informed, carefully considered and consistent with published research and with sound industry practice.

When setting up your scenarios or rules to be utilized in the automated transaction monitoring system, you should map the areas with higher ML/TF inherent risks to scenarios or rules to ensure there is coverage of such risks. When setting the thresholds for your scenarios or rules, it is important to consider conducting some level of statistical analysis of the percentage of coverage (i.e., customer or transactions that would be captured by the scenario) to determine whether the scenario will identify those customers and/or transactions that present the highest risk. When setting your production scenario or rule thresholds, it is important to consider the results of below-the-line scenarios as there may be potential suspicious activity below your threshold that may warrant the threshold of the scenario to be reduced to include suspicious activity that may have gone undetected.

In addition, you should consider historical suspicious activity experience within your financial institution. Also, it is important to remember that all scenarios and settings should be reviewed in a "test" environment before moving them into production to ensure that scenarios are operating as designed.

Once you have implemented your transaction monitoring scenarios or rules, it is important to maintain key performance indicators (KPIs), such as an alert to information request percentage, an alert to investigation percentage and an alert to suspicious activity report percentage, as this will assist the institution in determining the effectiveness of each scenario or rule on an ongoing basis.

Some common pitfalls that may occur when reviewing automated monitoring systems are:

- Inaccurate or incomplete model documentation
- New ML risks to the institution are not considered part of the transaction monitoring model
- Misaligned alerts to ML/TF risk profile (i.e., focus of scenarios or rules are for areas identified as low risk to the institution)
- High-risk jurisdiction alerts do not consider all countries involved with a transaction and redundant alerts or scenarios (i.e., looking at the same activity multiple times)

Financial institutions should look for opportunities to monitor transaction activity by customer peer grouping. This will allow for a more tailored transaction monitoring approach and it will allow an institution to benchmark customers against their peers and identify outliers that may present heightened ML/TF risk to the institution.

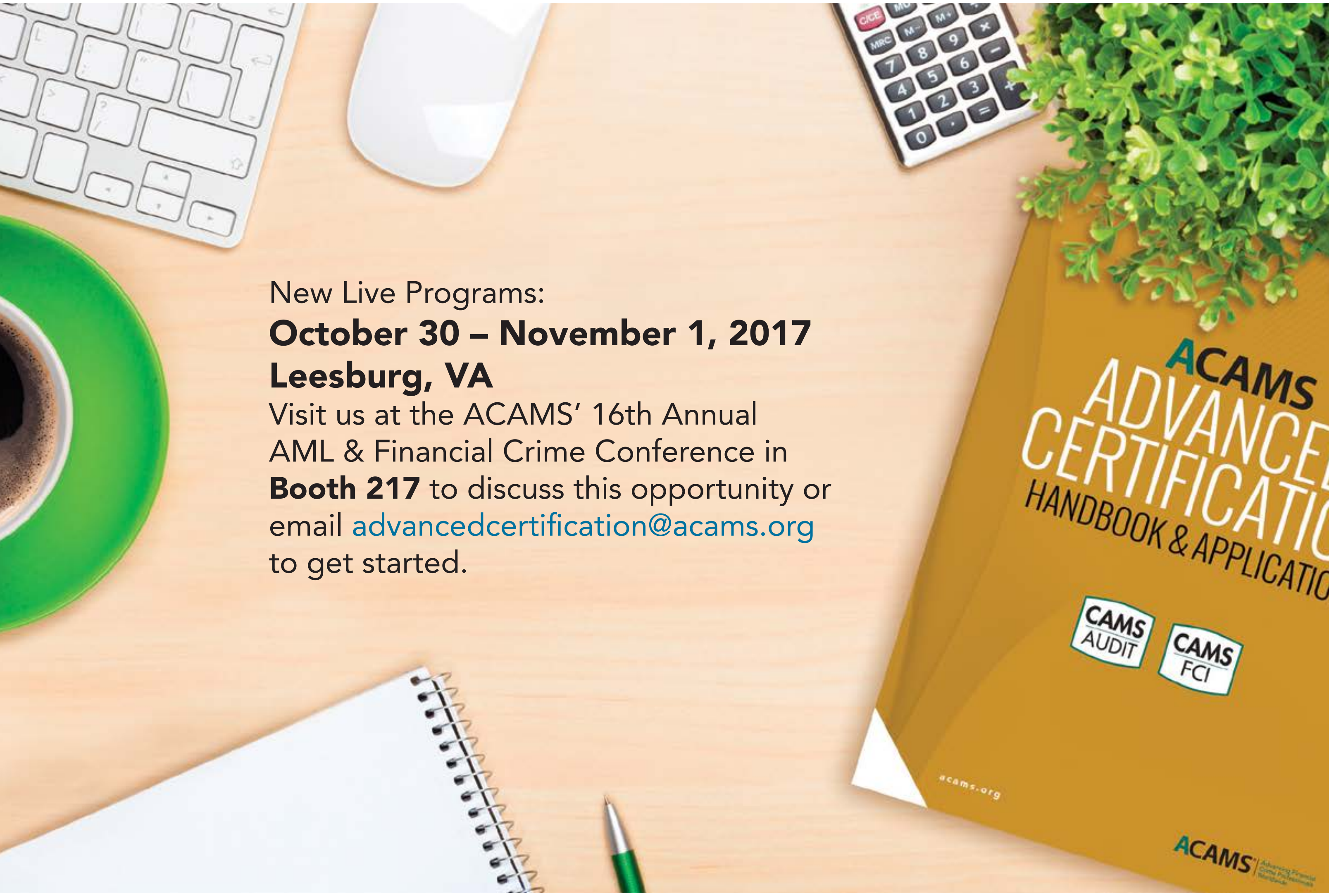
In the near future, at a minimum, institutions will need to consider creating a Model Governance Committee responsible for oversight of the institution's model, risk management program. Your financial institution should conduct an AML model inventory documenting all the systems utilized to monitor ML/TF risks within the institution. The Model Governance Committee should determine and document the frequency of any calibration and validation efforts.

In summary, a sound enterprise-wide risk assessment is the key to bridging the gap to effectively identify and monitor ML/TF risks within your financial institution. By setting up your compliance program in a manner commensurate with the institution's ML/TF risk profile, you will be able to focus your attention and resources on those areas that present the highest risk to your financial institution.

Jason Chorlins, CAMS, principal, Kaufman Rossin, Miami, FL, USA, jchorlins@kaufmanrossin.com

[3] "Supervisory Guidance on Model Risk Management (OCC 2011-12)," Office of the Comptroller of the Currency, April 4, 2011, https://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf

The ACAMS Advanced Certification live programs not only provide you with access to industry experts sharing their experience and knowledge and a class of peers to learn from and lean on throughout your career, but also the tremendous opportunity to become a published expert in your field — searchable, discoverable, recognizable.



New Live Programs:

October 30 – November 1, 2017
Leesburg, VA

Visit us at the ACAMS' 16th Annual AML & Financial Crime Conference in **Booth 217** to discuss this opportunity or email advancedcertification@acams.org to get started.

AML and Financial Crimes Professionals with ACAMS Advanced Certifications* are recognized as elite seasoned professionals with superior skills committed to and focused on growing professionally to benefit their institutions.

**You must be CAMS Certified in order to apply.*

CAMS AUDIT

ACAMS® Advancing Financial Crime Professionals Worldwide

CAMS FCI

The three building blocks of a centralized compliance system

When it comes to watchlist screening, what is at stake in today's high-risk business environment? Well, in 2016, nonbank institutions received 90 percent of all Office of Foreign Assets Control (OFAC) fines,[1] with 50 percent of those fines totaling $500,000 or more.

Those numbers are the most recent evidence of an emerging trend that poses a unique threat to these organizations. While sanctions screening fines have always been part of the regulatory environment, the upward trend indicates that OFAC is beginning to specifically target nonbank institutions, with insurance, logistics and money services businesses among the hardest hit. With this sobering thought in mind, these businesses must prepare their internal systems for increased regulatory scrutiny.

However, that is easier said than done. Many of these organizations have separate teams managing various functions, so sanctions screening efforts are tedious and manual. Furthermore, data streams flow into the organization and collect in disparate systems that never connect, and customer data resides in disconnected platforms that never merge for a consolidated customer risk profile.

But this problem is not specific to nonbanks. According to a recent ACAMS poll, 73 percent of the respondents said they use two or more solutions for automated screening. This might be one of the reasons why 58 percent of respondents said a regulator or internal auditor challenged their methodology for conducting a sanctions risk assessment.[2]

While every organization faces its own particular obstacles, they all face three main business challenges toward establishing a centralized compliance platform: creating a unified vision and corporate buy-in for compliance management; connecting disparate departments, systems and data feeds; and uniting all compliance functions into a single platform without having to start from scratch.

Creating a unified vision

As regulatory expectations increase, a constant tug-of-war ensues between an organization's compliance and operations groups. This necessitates a unified vision for managing compliance from an organizational perspective.

Naturally, the compliance group will have a lower risk appetite while remaining more averse to risk. For example, they will want the organization's compliance system to cast a wide net, identifying as many matches as possible. This requires a significant increase in the volume of data flowing through the system, as well as additional layers of oversight. However, this increase in volume creates a burden for the operations side, as extra layers of oversight require a steep uptick in the number of investigations of all of the additional matches.

Therefore, a consensus must be formed: Compliance and operations must come together to analyze data and metrics and to determine how to efficiently and holistically manage compliance. The result must instill confidence across business interests, from compliance to legal and the executive level, allowing each a customized view of their compliance data and common ground with which to make risk management decisions.

Connecting disparate systems

Unfortunately, many companies find that the responsibilities associated with compliance lead to a fractured internal compliance landscape; it is not uncommon for organizations to run multiple business functions that have separate compliance departments, processes and record management systems. While each department may have its own fully functioning sanctions system, their data may be inaccessible, incompatible or difficult to aggregate when a more comprehensive view or approach is needed.

[1] "Understanding OFAC: A Best Practices Compliance Guide for Businesses," CSI, http://csiweb.com/resources/white-papers/understanding-ofac-a-best-practices-compliance-guide-for-businesses?utm_source=Link&utm_medium=Article&utm_campaign=Acams_IDRiskHub_RC_06_FY18

[2] "The 2017 Hollywood Conference Polling Results Are In," *ACAMS Today*, April 24, 2017, http://www.acamstoday.org/2017-hollywood-conference-polling-results/

CENTRALIZED COMPLIANCE SYSTEM
01
UNIFIED VISION
02
CONNECTION
03
SINGLE PLATFORM

Furthermore, relationships that are identified as high risk in one compliance system might not receive the same scrutiny in a separate business function within the company if data sharing across systems is difficult or absent.

Uniting into a single platform without starting from scratch

An organization seeking to develop a centralized system must first answer a series of difficult questions: Does it currently manage its onboarding process, know your customer/risk profiling, transaction screening, watchlist updates and other compliance functions in a way that allows for easy aggregation and report generation? Does it rectify and navigate the competing interests among executive, legal, sales and compliance departments? Finally and most importantly, do all of those functions interact with one another?

Once these questions have been answered, the development of a centralized platform begins. Creating a completely new platform from the ground up is difficult, considering most companies have existing processes and platforms they do not wish to abandon. Few organizations have the time, money or programming resources to develop a centralized compliance system from scratch that can seamlessly bridge all the various compliance functions and datasets without affecting the end-user experience.

Therefore, the logical solution is to integrate a platform within the company's existing systems that merges all those disparate systems and processes.

The many benefits of a centralized compliance system

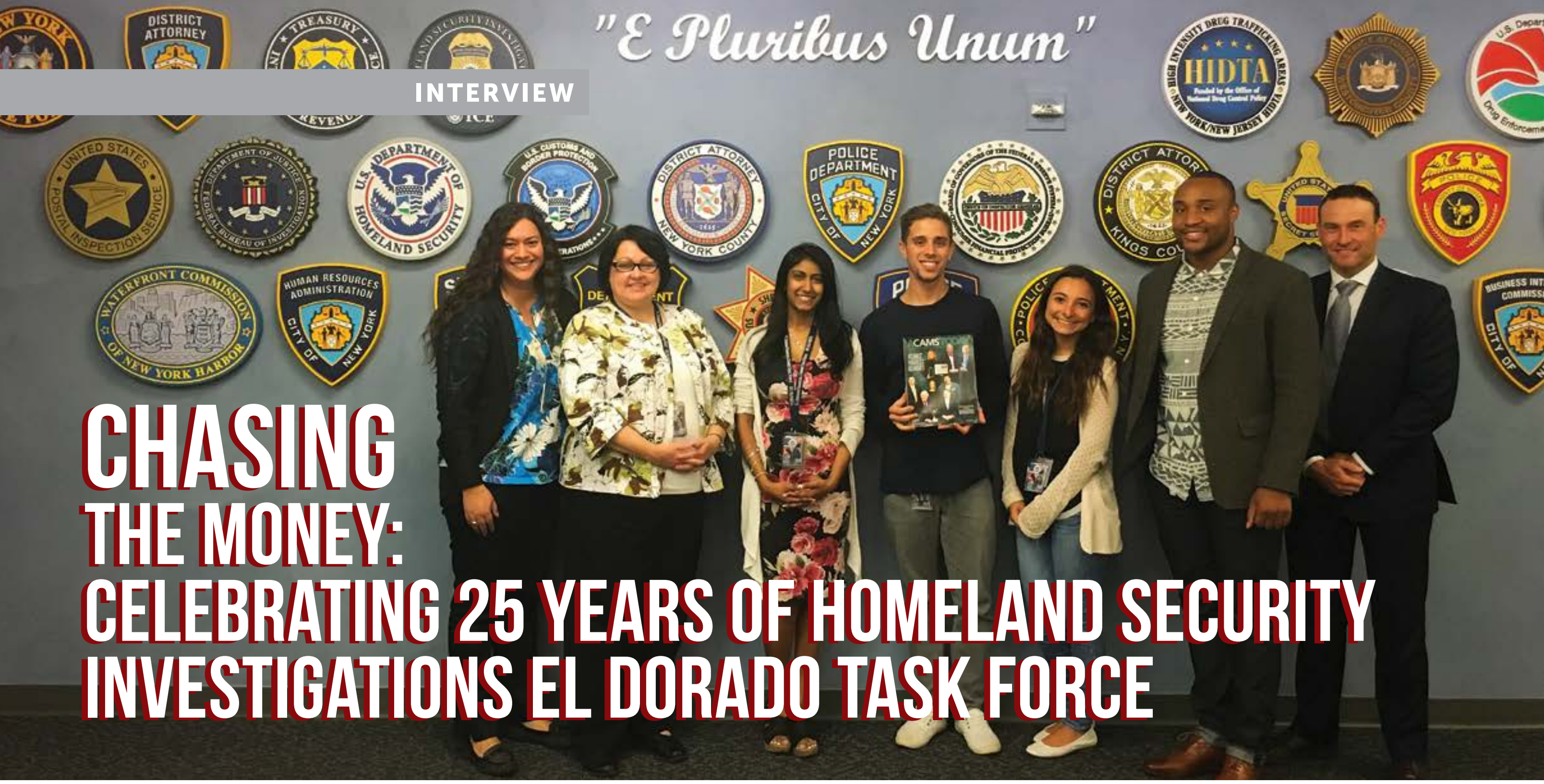
From an audit and regulatory perspective, a centralized system not only allows a comprehensive means to aggregate data on the results of sanctions activity, but also provides a view on both specific and overall compliance efforts, including policies, procedures and controls. In other words, a company should always be prepared to show auditors what they are doing in terms of due diligence, as well as demonstrate the rationale underpinning how they are doing it. A centralized platform is invaluable if a company is asked by regulators to provide documentation showing that it is following appropriate sanctions protocols to prevent risk and meet legal expectations.

There are also financial benefits to implementing a centralized compliance system. A Dow Jones and ACAMS study found that 40 percent of companies surveyed exited a full business line or segment of business in the prior 12 months because of the perceived regulatory risk or their inability to manage that risk.[3] With a centralized sanctions system in place, these regulatory risks become far more manageable, allowing companies to pursue and retain lines of business that would have otherwise been considered out of reach.

Pulling together the various components of an effective sanctions screening program can seem unwieldy. Building a platform from the ground up might be improbable for most companies, given the scope of such a project and the operational implications. So, identifying a third-party platform that can serve as an interlocking system for internal departments, systems and data feeds can be a more realistic option. In leveraging such a solution, organizations can create a holistic compliance screening platform that centralizes all compliance functions into a single view. A

Michael Brown, CAMS, vice president of product strategy, CSI Regulatory Compliance, Charlotte, NC, USA, michael.brown@csiweb.com

[3] "ACAMS and Dow Jones Anti-Money Laundering Insights Survey," 2016, http://www.acams.org/download-your-aml-resources/



CHASING THE MONEY: CELEBRATING 25 YEARS OF HOMELAND SECURITY INVESTIGATIONS EL DORADO TASK FORCE

Amidst the legions of buildings in Midtown Manhattan, New York City, sits an expansive, nondescript, yet historic redbrick building. From the outside, one would never guess that the 30 different agencies operating within the building comprise the Homeland Security Investigations (HSI) El Dorado Task Force (EDTF). HSI EDTF has been crime fighting for the last 25 years. They have cracked some notorious cases and brought down some infamous criminals. This year commemorates 25 years of fighting crime and many successes. *ACAMS Today* was fortunate enough to spend the day with HSI EDTF and to catch a glimpse of their fascinating crime-fighting world. What follows is a transcript of recollections, impressions and interviews from my day with what I consider some of the real heroes of New York City.

▲ Erik Rosenblatt, HSI EDTF assistant special agent in charge

As we approached the building in his vehicle, Erik Rosenblatt, HSI EDTF's assistant special agent in charge, pointed out that the parking level where we drove up was used in 2001 as the U.S. government's World Trade Center central command after the 9/11 terrorist attacks. The building covers an entire city block and back then there were not a lot of neighbors in the neighborhood. Things have definitely changed since then. Now, storefronts for numerous famous designers and brands such as Ralph Lauren and Martha Stewart line the block.

When we entered the building, I quickly realized how huge an entire New York City block really is. As we walked into the HSI EDTF headquarters, Erik told me, "Well, the first thing we need to do is get you a pass." We approached what I imagine was a bulletproof window and I was asked to turn over my driver's license. By the way, it did not matter that the person in charge of the HSI EDTF was standing right next to me; the gentleman at the window looked at my driver's license picture to make sure I was the same person standing in front of him. He then filed my driver's license and slipped my pass through the glass compartment. I was now an official guest of the HSI EDTF.

As the tour continued, Erik pointed to different hallways and explained where each one led. We went around a corner and reached his office. As he fired up his computer and we started planning the day, he told me that he had received word that there had been a big money laundering bust the night before and that there were three guests staying in the HSI EDTF hotel (holding cell). He asked if, during our tour, I would like to go for a visit. My response was a quick "Yes."

Erik dove right in and began to share HSI EDTF's mission, which is "To disrupt and dismantle transnational criminal organizations involved in money laundering and other financial crimes affecting New York, but our reach is worldwide."

HSI EDTF's mission seems simple enough, but when Erik began to describe the extent of HSI's responsibilities, which range from financial crimes, anti-gang enforcement, cybercrimes, narcotic smuggling/trafficking to human rights violations to name a few, I was left in awe of the many areas of expertise encompassed by one single task force (TF). In striving to fulfill their mission, HSI EDTF is comprised of 30 federal, state and local participating agencies and over 200 federal, state and local investigators, intelligence analysts and prosecutors. "EDTF would be near impossible to replicate, but we collaborate with other HSI offices and our federal partners all over the country, in addition to foreign law enforcement organizations, to support their ongoing investigations and to help grow their financial crime investigations and financial intelligence functions," Erik explained. The benefits of such a wide and diverse network of agencies and individuals is astounding. The size of the TF was reemphasized as we later walked through the office and passed a wall, which featured all of the official seals of the various agencies.

Erik went on to share the importance of deconfliction and how inter-agency communication within the HSI EDTF assists so that each agency is not duplicating efforts or arresting each other's undercover agents or ruining well-executed sting operations.

One thing that Erik mentioned that resonated with me is the business side of financial crime fighting. Due to the collaboration amongst all of the agencies, every time agencies pool their resources together, if assets are seized, each department participates in asset sharing to further assist in the fight against financial crime and other crimes that affect the partner agency's hometown, such as combating the heroin and fentanyl epidemic. I asked Erik what was the biggest asset he had confiscated. He told me the most exciting was a jet, but the biggest was a commercial building.

▲ Erik Rosenblatt sharing the importance of interagency communication and the business side of financial crime fighting

Erik went on to share that HSI EDTF is passionate about its outreach program Cornerstone. At least a couple of times a month HSI EDTF provides trainings for the community on what individuals can do to assist in the fight against financial crime. Erik said, "We have an open door policy. We want to work with people to solve crime." When asked why HSI EDTF has been so successful, Erik said, "HSI is a collaborative agency. This is why it works."

During the tour, Erik received word that it would be a good time to visit the holding cells. As we made our way down to the floor on which the cells are located, we passed a couple of high-end stores, a gym and some locals, who as Erik put it, had no idea what was behind the non-descript door. As I passed through that door, I started to think about all the cop shows I had seen on TV and wondered if those fictionalized events would bear even a passing resemblance to the reality before me. I was not disappointed. After many past discussions with various members of the law enforcement community of their daily activities, it was gratifying to see first-hand a part of the investigation process. In seeing the HSI EDTF agents at work, I gained a greater appreciation for everything they do to keep our cities safe.

After our sojourn in the holding cells, we continued the tour by walking to the other side of the office city block before returning to Erik's office where I would have the privilege of conversing with six members of the HSI EDTF.

Ryan Hill, HSI supervisory special agent

ACAMS Today: ***Could you tell me about your role and what you do on a daily basis?***

Ryan Hill: My group is tasked with looking at non-traditional money laundering investigations—so everything outside of narcotics money laundering. Currently, some of the investigations we are working on are Ponzi schemes, securities fraud, manipulations of securities and commodities. We have also targeted the proceeds of contraband, for example, cigarette contraband trafficking. This is an offense that is not typically prosecuted because it is difficult to get the requirements for it, but we have found that we can do undercover operations where we can get information from the organized network that is operating these rings of contraband cigarettes. For example, these organizations go to low-tax jurisdictions, like Virginia, to buy as many cigarettes as they can at a low cost. They then sell the cigarettes at a higher price in the Black Market, which allows for huge profits even though they employ couriers and runners to travel on the interstate. We have discovered that this type of contraband trafficking has been tied to Hawalas because criminals prefer to use illicit money laundering networks because they operate without any oversight. However, not all Hawalas are used for illicit money. Since illicit money investigations falls under our purview, a lot of our investigations have begun with illicit money movement. This is why many of our investigations have begun with a contraband cigarette trafficking investigation. For example, imagine that a state trooper in West Virginia has pulled over a courier, which then leads to a larger network dealing in K2 synthetic cannabinoid distribution. The K2 is so prolific it has melded into the contraband cigarette trafficking. We have noticed in our undercover investigations that the criminals do not want us to purchase K2 synthetic cannabinoid as much as they want us to sell them contraband cigarettes, so they can trade between contraband cigarettes from low-tax jurisdictions for K2. We are seeing an overlap between K2 and the contraband cigarettes and even though contraband cigarettes do not appear as a public safety, K2 is and the melding of the two is affecting the public safety.

▲ Ryan Hill, HSI EDTF supervisory special agent

AT: ***Would you say that it is related to synthetic opioids?***

RH: It has been related to fentanyl and synthetic opioids.

AT: ***Could you expand on your work with commodities?***

RH: We work closely with the Securities Exchange Commission (SEC) and we have recently started working closely with the U.S. Commodity Futures Trading Commission (CFTC). We worked on a case involving a woman that was a Harvard graduate and she played up her Harvard degree as a selling point to come across as a prolific trader. She even tried to say that she had an evolved trading rationale that would guarantee double-digit returns. She would take victims' money and prepare false investor statements and this was to the tune of $23 million. The SEC was the original provider, but the CFTC was the organization that we worked with to identify her and gather the evidence to obtain her conviction and we were successful.

AT: ***What has been your favorite case?***

RH: There was a Bangladesh organization made up of 15 to 20 individuals that had a very sophisticated way of conducting check fraud. They would create these high quality counterfeit checks and had access to great false IDs. They would then open bank accounts with banks and let them remain dormant for a six-month period. Because of the dormancy, the banks would relax their controls on these accounts. Then on a Friday, they would deposit a $15,000 check and would withdraw money from ATMs up to the ATM limits. They realized

◀ The seizure of $4.1 million

at some point that they could go to a casino and withdraw money to gamble. The casino would look at the customer's bank statement and note that they did have $10,000 available, so they would give the $10,000 to the customer. This process was repeated up to a million dollars and it was not until Monday that the bank's realized that the checks were counterfeit. And this was to the tune of $18 million.

AT: ***So how long was this fraud going on for?***

RH: This fraud had been going on for so long that the individuals we arrested admitted that they had inherited this scheme from a previous generation who had retired and handed over their skillset to the next generation.

AT: ***How did you get a break in this case or what led to the arrest of these individuals?***

RH: It was a piece of luck. It was a vehicle stop by the NYPD in Queens. The individual was stopped for a driving infraction, but the police officer noticed that they had quite a bit of checks and ID's in the car. This is an offense in the city of New York. The detective that went by had just spoken to someone in the EDTF about this and he was wondering if this was related to the discussion he had with someone in our office. The detective called up the bank investigator that was handling the case and the bank investigator put us in touch with him.

The individual was brought to the EDTF and we noticed that he had a key to a storage locker. We sent a couple of investigators to watch the locker. It turned out that one of the calls the detainee made, which was in his native tongue, was something to the effect of "go empty the locker." The locker was a treasure trove of documents that was needed for a conviction.

Bill Bronsteen, HSI special agent

AT: ***Could you tell me about your role with the HSI EDTF and what your team does?***

Bill Bronsteen: I am part of the undercover operations. This means we have informants in South America who work with money brokers. The money brokers set up meetings with drug dealers and money launderers for our undercover agents. Our undercovers are then put in contact with these money launderers. We pose as money launderers and conduct what is called 'money pickups' to further the investigation. The drug traffickers who launder their money are usually Colombians and Mexicans; however, the game has shifted in the last decade to Dominicans in Queens and a little bit of Mexicans in the Bronx and it has gone from cocaine to heroin. Although the players and drugs have changed, what hasn't changed is that the money is still going to Colombia and Mexico. Also, heroin has three times the street value that cocaine does; therefore, if criminals are going to risk their lives they are going to do it for heroin, where they can make three times the profit. The sad part is that 90 percent of heroin users were opiate users to begin with, but they have shifted over to heroin because it is easier to get and cheaper. This is a huge change from when I started my career.

AT: ***Your team arrested the detainees from last night that I visited earlier today with Erik at the HSI EDTF hotel, could you tell me what happened?***

BB: The detainees from last night were arrested for narcotics and conspiracy; however, we do know that one of them laundered money, but at this time, we are not charging him with that until we wrap up the case and then we can re-arrest them all on the money laundering charge.

▲ Karla Monterrosa-Yancey, *ACAMS Today* editor-in-chief and Bill Bronsteen, HSI EDTF special agent

So, that was last night's case; but, two days ago we had a money pick up and it worked just the way it is supposed to. We watched two guys deliver a giant duffle bag full of cash to a known associate of the organization but we can't hit the two guys because we have to protect our investigation. So, the two guys drove to another borough and someone delivered a bag to their car; however, the two guys are still off limits. So, we watched them drive to yet another borough and watched someone get into the car and leave the car with the bag. The guy who left the car is now free game. So, we were able to stop the guy and we discovered that the bag was filled with cash and the original two guys drove off and they never even realized what happened. In the end, by watching one target, we developed another target and we arrested him and seized the cash.

The interesting thing is that sometimes we will sit on a target for two months waiting for them to do the same exchange and they do not do it again. So, it does not always go as smoothly. Sometimes the criminals do the pickups every day and sometimes they do not do anything for months. This line of work is unpredictable.

Editor's note: Bill had been up for over 24-hours when I did this interview with him. He was also out with his team when they arrested the three detainees I had seen earlier in the day. He is only one example of the many dedicated people I met during my visit at HSI EDTF.

AT: ***What was your most memorable arrest?***

BB: Earlier this year we seized $4.1 million and three kilos of heroin. That case has generated almost $10 million in seizures in the last three years and 90 kilos of heroin and 18 arrests. We had a heroin seizure on that case two years ago that included 70 kilos of heroin and $2 million, which was the fourth largest heroin seizure in the country and the largest in the state of New York. The prosecutor said there was enough heroin in that seizure for every man, woman and child in New York to have a hit of heroin. So, it was rewarding to get heroin off the street. People ask, "Why fight the drug battle if you are not making a dent?" But you can make a dent. You are hurting the criminals financially. Stopping and dismantling is difficult, but slowing them down and getting them off the street makes a difference. Even though we are a financial group because we are doing narcotic proceeds, sometimes we run into narcotics by mistake and sometimes we will seize more by mistake than some street cops will seize their whole careers because we are trying to get the dirty money off the streets and then we get to prosecute the criminals.

▲ The three kilos of heroin

AT: ***Do you have cases that go national or extend to other states?***

BB: Yes, our drug trade teams come from Texas or Miami, Boston and Rhode Island. We deal mostly in the northeast and down the coast, but we have had some cases that have extended to California. For example, cocaine was being bought and shipped to California and to Canada, but since we focus on New York, we call the other offices in other states and send them our leads.

AT: ***What are other ways you follow the money besides your own covert operations?***

BB: We work together with the different groups in HSI EDTF and we also do a lot of surveillance. It is extremely rewarding when we get the people arrested and prosecuted. For example, we had been surveilling the target from last night for six weeks, and when we stopped the suspect yesterday, the bag they had was empty. So, the next step was to search the car for money traps. We had a dog come and the dog confirmed that there was a scent of narcotics. So I ripped up the front seat cover and inside the front seat was a hidden compartment where the drugs were hidden. Everything is about hidden compartments. The interesting thing is that the driver gave us consent to search his car. Guilty people seem to want to be cooperative and they never think we will find anything. Criminals spend a lot of money outfitting their cars and homes with hidden compartments. The $4.1 million was all hidden in furniture.

AT: ***What has been your longest and shortest case?***

BB: Four years and still ongoing is the longest case. The target is smart enough to never touch the money. So, I would like to catch that target before I retire. The shortest case was an hour.

Editor's note: After the interview, Bill went back to work to continue his 24-plus hour shift.

▲ The commercial building seized by Erik Rosenblatt

Myles Mahadi, NYPD detective

AT: ***What does your day entail?***

Myles Mahadi: A lot of paperwork. The NYPD organized crime investigation unit is a very proactive unit because we initiate investigations. I also have a strong background in money laundering, specifically cases dealing with human trafficking and high-ring prostitution. When I arrived at HSI EDTF, I saw that no one specialized in these cases even though they were textbook money laundering cases. I am a subject-matter expert, much to my mother's embarrassment, on high-end prostitution. It is a very interesting and unique sub-culture, particularly when you talk about money laundering and financial crimes. In my opinion, it has not received the exposure it should. There are two things that the sex industry relies on, one is advertising and the other is banking. The advertising is easy to stop.

AT: ***ACAMS Today has published articles on this topic, there have been sessions on human trafficking at ACAMS conferences and the response is always the same, people want to know what else can they do to help in the fight against human trafficking?***

MM: They need to monitor more. For example, I presented at the annual El Dorado Task Force/High Intensity Financial Crime Areas (HIFCA) symposium where I went over how we would investigate a human trafficking case as a paper case. Toward the end of my presentation, I pointed out that when we arrest the owners of these human trafficking syndications, they always lead to other arrests or other cases. For example, HSI EDTF arrested a former NYPD officer as part of a crime family for a gambling charge. Incidentally, he was just arrested again for a bank mortgage fraud violation the other day.

AT: ***In the cases you have worked, are the victims of human trafficking local or international?***

▲ Myles Mahadi, NYPD detective

MM: There are two things two consider when chasing human traffickers. First, there has to be a base for the traffickers to set up shop (e.g., the Asian massage parlors or escort agencies). These girls come to a new country and then that is it. The human traffickers have certain terms like the Korean express or the Chinese express and you will find the victims in all parts of the country working. There is an organization behind all of this and the smart approach is for law enforcement and financial institutions to partner up and work together to resolve this. For example, how can we identify these human trafficking organizations? A human trafficking organization is not going to walk into a bank and open an account under ABC Escorts because no bank is going to tolerate this. However, if they walk into a bank and open an account under ABC Consulting LLC that they set up two weeks ago, the human traffickers now have a bona fide entity. And in my cases, that is the essence of money laundering because once the funds start to go through the entity that was created solely to conceal what the source of the funds is, then it is good to go. These human trafficking cases are textbook money laundering cases, but they are also very tight prosecution cases. The key element to getting these cases solved is aggressive prosecution. Second, many of these girls are transported across state lines. Another side to this is that many of the escort agencies are fronts for narcotics trafficking and frankly, there are loser men out there that call up these salons and order drugs and the girl delivers the drugs. If the girl does not have to have sex with the man then it is also a win for the girl and that is the way they look at it. It is an interesting sub-culture.

AT: ***Could you speak more about the financial aspect of the narcotics delivery side of human trafficking?***

MM: Well, for example, if I owned a high-end escort agency my line to the women would be let's get as many billable hours as we can, especially if I am sending them out to deliver drugs. For example, one of the things that I discuss during my presentations is to pay attention to multiple charges that occur on one credit card in the middle of the night. It would be suspicious if the company that is processing those charges is ABC Transportation Inc., in New York, but all those transactions are off by a dollar or two dollars because they want to trick the credit card software. So, the way it works is that when the girl arrives at the hotel room she asks the John for a driver's license, another form of ID, a credit card, and to sign a verification slip. So the John does all this and the reason for this is to fight charge backs on the credit cards. And this all gets processed and it gets keyed in. All the charge backs are carbon copy slips. This is a great tell to know that this is a human trafficking organization. The owners of the trafficking rings do not want to give the girls devices that they can use to swipe the cards on because the owners want complete control.

AT: ***What was your most memorable case?***

MM: A previous federal case called NY Confidential. The case took place in 2005-2006. The pimp's name was Jason Itzler, aka, the King of all Pimps. He graduated law school and got into the sex trade and had his office right next door to 26 federal plaza, which is the home of the FBI in NY. He went from making $60,000 a month to $450,000 a month in six months and no one noticed. We prosecuted Paul Bogrine and he got RICO-ed[1] in Newark by the FBI. He is currently serving six life sentences, plus 20 years for murdering witnesses and for witness intimidation. These cases always lead to other things and there is always something else.

Karla Monterrosa-Yancey, *ACAMS Today* editor-in-chief

Donna Luisi, HSI EDTF senior intelligence analyst, Financial Intelligence/HIFCA

Margret Marnell, HSI EDTF program manager, Financial Intelligence/HIFCA

Donna Luisi, HSI EDTF senior intelligence analyst, Financial Intelligence/HIFCA

Margret Marnell, HSI EDTF program manager, Financial Intelligence/HIFCA

AT: ***Donna, what is your role with the HSI EDTF?***

Donna Luisi: As the senior intelligence analyst for HSI, I have done several things with HIFCA over the years. I used to be in charge of SAR reviews. Now I am in charge of case support. What this means is that we receive a lot of requests from HSI EDTF agents and I work with our analyst to make sure they are doing the correct type of research and financial analysis, data visualization and putting it into a format that is understandable for everyone and appropriate for trial. One of our analysts recently went to testify at a trial. I have done threat assessments as well.

AT: ***Margret, what is your role?***

Margret Marnell: I am the program manager at HIFCA. My job is similar to Donna's. We function as deputies to Bill Macintosh, who is the supervisor of HIFCA. I work with the analysts specifically in complex multi-targets and strategic investigations. For example, I work on projects where we are pursuing a specific theme or issue rather than just an individual target set.

AT: ***Margret, what led you to join the HSI EDTF?***

MM: I started in Washington, D.C., where I worked in the Treasury Department in the office of Intelligence and Analysis and prior to that I worked for the Department of Defense as a weapon's analyst. The Treasury Department of Intelligence and Analysis is a sister office to OFAC, FinCEN and TFC.

[1] This is a term used by law enforcement. It is referring to the Racketeer Influenced and Corrupt Organizations (RICO) Act, a "U.S. federal law that provides for extended criminal penalties and a civil cause of action for acts performed as part of an ongoing criminal organization."

After moving to New York, I was happy to be able to join the HSI EDTF and to see a different side of the illicit finance coin. In my previous job, the focus was on national security threats and international financial flows and that has been helpful for me in working with the types of cases that HSI EDTF receives. Working here has given me more exposure to the domestic side and the private sector.

AT: ***Is there anything peculiar or interesting that your analysts have found in a SAR?***

MM: It is hard to pick just one because every SAR that turns into a referral has interesting aspects of their own. Analysts have worked on SARs that end up plugging into complex money laundering investigations or you will find a SAR that on its face does not appear very interesting that might be run of the mill narcotics related or a very low-dollar amount. But once you start putting the pieces together, it ends up leading you to a multi-million dollar trafficking network that expands across multiple states.

DL: In other words, something small can lead to something big.

AT: ***Do you use SARs to identify and choose your strategic investigations?***

MM: Yes, SARs are our main source of information.

AT: ***Do you have any tips for financial professionals when they are filling out their SARs?***

DL: Yes, we do quite a bit of community outreach through our Cornerstone program. We visit different financial institutions and we do training on how to write SARs better and on what we look for. We answer the who, what, where and how. We scan and target for certain terms. For example, writing down if the crime is human trafficking, narcotics related, or terrorist financing is helpful. The most important thing is being succinct. It is also important to include updated contact information because we do follow up and reach out to the banks for more information.

AT: ***What are the most common questions you receive when you are doing the training for financial institutions?***

MM: The biggest one is what do you look for when reviewing SARs.

DL: HIFCA, in conjunction with HSI EDTF and the Federal Reserve Bank, sponsors a financial symposium. We have had panels on Fintech and blockchain technology. We invited over 300 people from the financial sector and law enforcement. This is a great opportunity for outreach. We also do the international leadership program through the state department. We have many leaders come in, such as top-level financial ministers and prosecutors from different countries, and we have discussions on how to foster better partnerships between the public and private sectors.

MM: One of the messages we want to get out to the financial sector is please do not be afraid to contact us.

Interview with undercover agent

I had the opportunity to meet an undercover agent while I was visiting HSI EDTF. For the purposes of this interview, we will call him Zachary. I have met a couple of undercover agents in the past, but I have never had an opportunity to sit down one-on-one and ask them questions.

When Zachary walked into the room, he was not what I expected. Zachary was all smiles and seemed like he had been working at a desk job his whole life, but the truth is that Zachary was recruited his senior year of college and has been an undercover agent for almost two decades. He has been all over the world and has handled cases in many jurisdictions. In fact, when I spoke with him he was handling at least ten sources in multiple countries. Zachary was able to share that many of his cases dealt with narcotics, smuggling and money laundering. He modestly stated that through his efforts, his team and his confidential informants (CIs), he has been able to catch a few bad guys and break up some smuggling rings.

I, of course, wanted to know if he could share a war story where he faced immediate danger. He graciously obliged and told me about his experience when meeting a drug dealer. The dealer was known to be violent and unpredictable. They scheduled to meet in an open field and the agent had plenty of back up. However, as he drove up to the field for the meeting, the surveillance helicopter kept getting too close and the agent had to wave them off more than once. As he arrived to the rendezvous already worried about his cover, the agent saw that the dealer was waiting for him. He got out of the car and approached the dealer. They started speaking and the dealer asked the agent to follow him to the rear of his car. The dealer opened the trunk and on top of some bags he had a machete. The dealer leaned into the car and began to stroke the blade of the machete with one hand. The dealer asked the agent if he was a cop and if the agent was going to betray him. The agent remained cool but knew if he gave the wrong response, his back up was too far away to prevent anything. The dealer was satisfied with the answer and they concluded their business.

Zachary later testified against the drug dealer and the drug dealer could not believe that Zachary was indeed an undercover agent after all.

Zachary like everyone else I met that day at HSI EDTF is passionate about what they do and I believe that the people and their passion is the secret to the TF's success. Happy 25th HSI EDTF!

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

USING DATA ANALYTICS TO IDENTIFY AML RISK

Data is the lifeblood of financial institutions and other organizations. It is used to run processes, manage financials, predict risk, prove compliance, target customers and influence decisions. In anti-money laundering (AML) and compliance, the data required to identify and combat financial crime is complex. It is also difficult to gather because data is often stored across a patchwork of legacy systems, new systems and siloed business-specific applications. Data quality can vary greatly. Working with unreliable, incomplete or inconsistent data makes it difficult to identify bad actors who pose a financial and reputational threat, which undermines an institution's ability to efficiently manage risk across the enterprise.

The more complex and geographically diverse a financial institution is, the greater the threat. Institutions with very large customer databases and transaction volumes that span numerous distribution channels and counterparties face the greatest number of challenges and the most risk.

The slinging arrows of risk

Traditional AML defenses that rely primarily on static rules to identify questionable individuals and activities are coming up short. Despite continued investment in AML technology and processes, institutions seem unable to keep pace with external threats from drug cartels, corrupt public officials, terrorist organizations and other bad actors that have developed increasingly sophisticated tactics to avoid detection. These savvy criminals know how to play the game. They will often cloak their malicious activities by keeping within the defined set of rules. One example of how criminals fly under the radar is through smurfing. By limiting transactions to under $10,000, they avoid triggering a currency transaction report.

Internal threats—whether unintentional human error or intentional fraud—must also be considered when managing enterprise risk. In addition to internal and external threats, emerging payment technologies and the digitalization of banking have introduced yet another set of risks to the AML landscape.

INTERNAL THREATS—WHETHER UNINTENTIONAL HUMAN ERROR OR INTENTIONAL FRAUD—MUST ALSO BE CONSIDERED WHEN MANAGING ENTERPRISE RISK

Cyber risk, social media monitoring and data management are all crucial considerations that have caught the attention of regulators, who have come to recognize that traditional, rules-based methodologies may not be optimal for certain typologies. Check-the-box compliance is not enough. Regulators expect banks to have defensive processes and systems in place to proactively seek out and catch perpetrators, whether external players or internal employees.

Big data, big challenges

Know your customer (KYC) regulatory requirements have compelled institutions to collect increasing amounts of data on customers and their transactions. Static, rules-based systems are not designed to handle huge stores of unstructured, internet-scale data. As a result, they produce an enormous volume of false positive alerts. More data only produces more false positives when screening for sanctioned entities or money laundering.

Managing the deluge of false positive alerts is a major pain point for many institutions. Not only is the process inefficient and operationally expensive, but it complicates an institution's ability to quickly and accurately identify risk. The knee-jerk reaction of "throwing more bodies" at the problem is not the answer. Adding resources just drives up the cost of compliance and increases the risk of human error.

Driving change

The big data phenomena brought a proliferation of technology that can help meet the analytic and architecture challenges of AML, KYC and counter-terrorist financing. Data science, data analytics and other advanced technologies like artificial intelligence (AI) and machine learning offer a dynamic approach that is better suited to complex internet-scale data than static models. According to a report published by Celent, "AI-enabled solutions can not only automate significant parts of operations but also offer superior insights through advanced capabilities for analyzing structured and unstructured data."[1]

These dynamic models focus on patterns rather than individual data points or transactions. They detect anomalies, making it easier to identify behavior that truly accounts for malicious activities. Dynamic models enable institutions to keep pace with changing requirements while also resolving the costly problem of reducing false positives.

Integrating non-traditional data sources into a data management program will improve the effectiveness of detection and ongoing due diligence. Non-traditional internal and external data sources can include documents, newsfeeds, images, video, social media, clickstream data and machine log data. Driving the growth of these variable data sources are an increase in client interactions and the digitalization of business processes.

While these new data sources offer a wealth of information for AML and compliance purposes, traditional structured query language-based analytic techniques may not be well suited for these non-traditional data sources because their pre-set schemas vary and change often. For this reason, an alternative approach for analyzing data uses programming languages such as Java, Python and R. These coding languages are often chosen for big data and analytical tools for several different reasons. For example, Python has become a popular choice for applications because it relies on the most cutting-edge techniques, such as AI, machine learning and natural language processing.

The ability to integrate non-traditional internal and external data sources enables institutions to go beyond basic analytics to identify risk more quickly and efficiently. When transaction data is enriched with client/legal entity data (including names, addresses and other identifiers), and publicly available OFAC lists, banks can track transactions to determine if they were completed by known high-risk individuals or non-cooperative jurisdictions. Going one step further, enriching this data with verbal and written communications information can help cast a wider net when looking at potential indicators.

Tip of the iceberg

Fighting crime with big data and analytics still has a long way to go. Industry pioneers who wish to move beyond analytic technologies are looking toward cutting-edge solutions based on probability and inductive, heuristic logic that detects money laundering by replicating an analyst's thought processes. This is the future state of advanced capabilities that institutions require to address comprehensive AML and compliance challenges in a dynamic environment. With the right investment in the right technology and data platforms, institutions can be confident that they have a clear view of risk across the enterprise.

Carol Stabile, CAMS, chief sales and marketing officer, Safe Banking Systems, Mineola, NY, USA, carol.stabile@safe-banking.com

[1] Arin Ray and Neil Katkov, "Artificial Intelligence in KYC-AML: Enabling the Next Level of Operational Efficiency," Celent, August 22, 2016, https://www.celent.com/insights/567701809

Deconstructing a fraudster

What part of committing fraud is a good idea? For fraudsters, in the short term, the answer is everything. However, in the long run, the answer is nothing. The reason for this is that over time the weight of deception will cause a fraud to collapse. On the surface, a fraudster has the advantage of being proactive in building their spin and deception. Invariably, they succeed at exploiting the window of opportunity to sell their fraud scheme to their victims. Below the surface, as the threads of fraud are pulled and unraveled by either victims and/or investigators, the fraudster is at a disadvantage because the window of opportunity closes and the deception is exposed.

If fraud is ultimately destined to collapse and fail, why do people commit fraud? The answer is that, for whatever reason, they do not consider the consequences of their actions or they do not believe the consequences apply to them. If individuals inclined to commit fraud understood that inevitably they would actually deal with the consequences of their fraudulent actions, and that such consequences would be negative, they would more likely be deterred from committing fraud.

Deconstructing a fraudster to prevent and/or disrupt fraud requires understanding. You must understand the fraud risk, the mindset of a fraudster, the attributes of a fraudster, the fraud crime problem and the consequences of fraud. When you can place risk, mindset, attributes, the crime problem and consequences in context with each other, you can develop detective and preventive measures to deconstruct a fraudster.

Understanding fraud risk

In our personal and professional lives, we are all susceptible to falling victim to fraud for a variety of reasons. We tend to be gullible about “too good to be true” schemes and are prone to lack situational awareness for the warning signs of fraud. The three basic risks that drive fraud are the following:

1. Trust
2. Lack of control mechanisms that provide opportunity
3. Lack of deterrence or understanding about consequences

Trust is the foundation for building personal and professional relationships. Trust is also a fraudster’s best friend. Trust facilitates opportunity because it enables a fraudster to circumvent control mechanisms. Misplaced trust buys time for a fraudster to keep the window of opportunity open and to perpetuate their deception. Differentiating between meaningful relationships and fraud requires understanding and situational awareness. Understanding the motivation and rationalization used by fraudsters to justify their actions can be a critical component in recognizing the risk of fraudulent behavior.

Situational awareness is being aware of your physical surroundings. It requires being vigilant in identifying potential threats and dangerous situations. According to Stratfor, a leading geopolitical intelligence service, being situationally aware of your physical surroundings is more of a mindset than a skill. It is the recognition that threats exist and taking responsibility for your personal security. One of the key best practices is to trust your gut or intuition. If a person or activity is out of place or unusual, trust your instincts and be attentive for potential danger.

The same concept about situational awareness can be applied to fraud. It requires being vigilant in identifying and mitigating potential fraud risks and schemes. Being situationally aware of fraud is more of a mindset than a skill. It is the recognition that you are constantly vulnerable to fraud. You have to accept responsibility for your fraud vulnerability. The key best practice is to maintain your objectivity about trust, reasonableness and temptation. You must be objective about establishing trust relationships and not allowing such relationships to circumvent control mechanisms, such as separation of duties. You must consistently assess the reasonableness about situations and scenarios with which you are presented. You must remain objective about being lured into the temptation of financial enrichment or a false sense of security to scenarios that sound “too good to be true.”

Strong control mechanisms and monitoring limit the opportunity to commit fraud and lead to fraud deterrence. A perception of detection is more likely to cause a potential fraudster to consider the consequences of their actions. If an individual thinks that internal controls are in place that will detect fraud, they will be less inclined to “cross the line of integrity” and commit fraud.

Understanding the mindset of a fraudster

I have investigated fraud for 45 years and I have been teaching fraud awareness since 1981. In my experience, a fraudster’s mindset is driven by five factors. Those factors or elements are as follows:

1. Integrity
2. Opportunity
3. Incentive or pressure
4. Rationalization or attitude
5. Capability

The five factors or elements build upon each other. An individual’s integrity is the starting point. If a person possesses a great deal of integrity and has limited opportunity,

FRAUD

they will be less likely to cross what I refer to as "the line of integrity" and commit fraud. Conversely, if a person possesses limited integrity and is afforded a great deal of opportunity, they will more likely cross "the line of integrity" and commit fraud. In many instances, the integrity and opportunity continuum falls between the two extremes and will be driven by a combination of the other three factors: incentive, rationalization and capability.

Opportunity, incentive and rationalization are referred to as the fraud triangle. They were introduced in 1953 by criminologist Donald R. Cressey. The fraud triangle became widely recognized in the mid-1970s. The combination of the three factors was believed to be the drivers that led individuals to commit fraud. Opportunity represents the chance to commit fraud. Incentive or pressure represents the motivation and is usually caused by financial demands. Rationalization or attitude is the self-justification making the fraudulent act acceptable.

Subsequently, in 2004, David T. Wolfe, a certified public accountant and forensic accountant, and Dr. Dana R. Hermanson, a college accounting professor, published a paper, which added capability to the fraud triangle, creating the fraud diamond. They believed that unless an individual possessed the right capabilities, they would not succeed in committing fraud. Capabilities are the personal traits and skillsets necessary to exploit opportunity, incentive and rationalization.

Opportunity is the most important factor because it influences integrity and capability. If there are strong control mechanisms and a perception of detection, there is limited opportunity. Limited opportunity would then be more likely to deter an individual from crossing "the line of integrity." Likewise, regardless of the proficiency of skillsets, the prospect of detection would likely serve as a deterrent.

When an individual succumbs to the temptation of committing fraud and crosses "the line of integrity," what do they think about? They think about executing their fraud scheme without being detected. They think about establishing and maintaining their illicit funding stream. They think about protecting their illicit funding stream and personally benefiting from it. Fraudsters who think about the potential consequences of their illicit activity, particularly the ones who believe that consequences do not apply to them, will likely have an exit strategy. They recognize that their fraud scheme will have a useful life that will expire. These fraudsters tend to be more arrogant and lack empathy. For the most part, they are focused on identifying the warning signs that their fraud is about to collapse. If they are not overcome by greed—which happens in many cases and causes them to lose focus and get caught—they will attempt to execute their exit strategy, escape and protect their illicit proceeds.

FRAUDSTERS UNDERSTAND HOW TO USE FINANCIAL INSTITUTIONS TO FACILITATE THEIR ILLICIT ACTIVITY

Understanding the attributes of a fraudster

Looking back at the mindset of a fraudster, their attributes will be shaped, in part, by the combination of the fraud diamond and the specific fraud in which they engage. Once they exploit the opportunity, plan their illicit activity and cross "the line of integrity," their actions will be driven by the level of incentive required, in most instances, a financial incentive. As the opportunity and incentive come into focus, they will rationalize and justify their behavior. They will typically ensure they possess or acquire the necessary skillsets (capabilities) to achieve their illicit objective.

With the five fraud elements in place (integrity, opportunity, incentive, rationalization and capabilities), the attributes required to succeed manifest themselves. The fraudster must be motivated. They will be driven, manipulative and endeavor to develop and exploit trust relationships. They will need to be an effective communicator and effective self-promoter. They will usually start out focused; however, their focus could become blurred by a sense of greed and arrogance. Greed and arrogance can be a fraudster's ally or biggest adversary by evolving into a critical vulnerability.

In many situations, fraudsters will lack empathy toward their victims. This lack of empathy is one reason why fraudsters may be inclined not to consider the consequences of their actions. Fraudsters will endeavor to avoid detection and maintain focus. Maintaining focus will enable them to execute their exit strategy. However, their greed and arrogance can also cause them to lose focus and not recognize the warning signs of their demise. The lack of empathy and focus caused by greed and arrogance will frequently be the lynchpins to a fraudster's undoing.

Understanding the fraud crime problem

Fraud is deception. Fraud knows no boundaries. Fraud schemes range from simple to complex. Fraudsters are adept at exploiting systemic vulnerabilities, such as the anonymity afforded by the internet. Troublingly, fraudsters understand how to use financial institutions to facilitate their illicit activity. There has been an upward trend in civil litigation cases where victims and/or groups of victims of fraud schemes have sued financial institutions for their role in facilitating the fraud. In almost all such situations, financial institutions have been unwitting facilitators. Nonetheless, they find themselves subject to lawsuits.

Since there is an expansive range of fraud schemes, fraud should be assessed, understood and addressed from two perspectives or levels: generic and specific. The ability to be deceptive and avoid detection is a fraudster's primary key to success. When potential victims and investigators understand how fraudsters take advantage of generic and specific fraud schemes, they position themselves to more favorably deal with the situation.

From a generic or simplistic perspective, fraud is deception. Over time, the weight of the deception will cause the fraud to collapse. How long does it take before a fraud collapses and is detected? It could be right at the start. It could be a matter of days, weeks, months or years. The useful life of a fraud is contingent on numerous considerations. The more situationally aware you are regarding the risk of fraud, the more likely that a fraud can be prevented or detected sooner rather than later.

There are a variety of specific fraud schemes that range from investment fraud to corporate fraud, embezzlement, check fraud, elder fraud and so many more sham activities. Regardless of the scenario, it should be viewed as deception and then from the type of specific fraud scheme it is. You need to consider which specific fraud schemes you are more susceptible to from both a personal and business perspective. Common themes to assess will originate with the potential abuse of trust and circumvention of control mechanisms. Regardless of whether it is an investment fraud, business fraud, embezzlement, elderly fraud or a check fraud, the abuse of trust and circumvention of controls will likely be a factor.

Disruptive and preventive measures leading to the deconstruction of a fraudster

Deconstructing a fraudster requires proactive and reactive measures. Preventive steps will be more proactive and detection mechanisms will be more reactive. Deconstructing a fraudster begins with fraud prevention. The best form of prevention is deterring a potential fraudster from crossing "the line of integrity." To do so, build a perception of detection by minimizing opportunity and reinforcing the fact that a fraudster will face serious consequences for their illicit activity.

Best practices to limit opportunity include having strong internal controls, consistent monitoring and a fraud risk assessment, assessing and testing the trust environment, and overall vigilance and situational awareness. In a business setting, promote a no tolerance for fraud policy. This begins with the tone at the top of the organization. Business leaders must endorse strong ethical standards and embrace a no nonsense, no tolerance policy.

If you are reacting to a fraud that has been detected, deconstructing the fraudster starts with planning. You must assess the situation and prepare a written plan to address the fraud. Depending on the circumstances, you should determine how to exploit the vulnerabilities of the fraudster and how to develop evidence regarding the fraud. This requires understanding. The greed and arrogance of a fraudster cannot only cause them to lose focus, but it could cause them to more openly talk about their scheme and add additional layers of spin and deceit. The added spin and deceit adds additional weight to the fraud leading to its ultimate collapse. In addition, many fraudsters want you to know they are the smartest guy or girl in the room and they will not shy from talking about it. Be a good listener and let them talk and implicate themselves.

Other steps you need to consider in furtherance of deconstructing a fraudster includes not allowing the fraudster to gain the upper hand. Planning and preparation can assure that you maintain the upper hand. You must gather your facts objectively, be persistent and be analytical in evaluating the information you gather and assess the reasonableness of the situation. Another element to consider when planning is to develop contingencies to deal with potential exit strategies the fraudster might contemplate. Depending on the circumstances and the specific mindset of the fraudster you are dealing with, you can be confronted with a variety of potential exit strategies. Understanding and planning are the keys to deconstructing a fraudster.

Understand the consequences of fraud

It is important to recognize and understand the multiple consequences of fraud. All actions or inactions regarding fraud have consequences for victims, financial institutions and other third parties, as well as to the fraudsters themselves. Victims of fraud face financial loss, potential devastation and emotional distress. Financial institutions and other third parties could find themselves in the contrasting situation of serving as a facilitation tool or being a detection mechanism. Regardless of whether they find themselves as a facilitation tool or detection mechanism, they could face the consequences of financial, reputational and/or litigation risk. Invariably a fraud will collapse. Fraudsters face the consequence of prosecution and incarceration, restitution, seizure and asset forfeiture. In addition, fraudsters face the loss of family and loved ones as a result of their fraudulent behavior. The more that can be done to publicize and visualize the negative consequences fraudsters face, the greater the possibility of deterring potential fraudsters from crossing "the line of integrity."

Conclusion

What part of committing fraud is a good idea? If fraudsters were truly aware of the inevitable negative consequences of their illicit actions, they would more likely be deterred from fraudulent behavior.

Trust is the foundation for meaningful relationships. Trust is also a fraudster's best friend. Develop situational awareness for fraud with a focus on trust. Do not allow trust to negate control mechanisms. Limit the opportunity of fraud from occurring. Perception of detection is significant fraud deterrence. Strong internal controls will limit the opportunity for fraud. In promoting a perception of detection, reinforce the negative consequences of committing fraud. If a potential fraudster considered the inevitable negative consequences of fraud, they would likely be less inclined to cross "the line of integrity" and not commit fraud.

Once a fraud is occurring or has taken place, deconstructing a fraudster comes down to understanding and planning. You must understand the fraud risk, the mindset of a fraudster, the attributes of a fraudster, the fraud crime problem and the consequences of fraud. Understanding all of these should lead to better preparation and planning, which will subsequently lead to disruption and prevention. A

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

CONFIDENTIAL *congratulations*

Feedback and "war stories" from successful suspicious activity report (SAR)-based investigations are an often sought topic for ACAMS articles, conferences, seminars and presentations. Although general validation of the value of anti-money laundering/Bank Secrecy Act (AML/BSA) programs are regularly touted by law enforcement representatives, specifics are rarely cited. Even if it was practical to give confidential congratulations, it is a consideration rarely recognized by those in the actual position to bestow them.

Your AML alert software culls a customer from out of the data stream. Your job in BSA/AML compliance is to review these types of anomalies and decide if it is worthy to file a SAR. All the identified indicators are consistent with your AML training and experiences and constitute near textbook examples of suspicious transactional activities. The kind of activities any regulator would consider a "no-brainer" for a SAR filing.

A couple of months later, somewhere at a SAR Review Team far away, that well-articulated, brief and concisely written SAR grabs the attention of an agent reviewing a recent download. The address also catches the agent's attention. This is an area the agent is familiar with and where other "front" businesses have been found to be covering for illicit activities. The agent knows that the amounts outlined are inconsistent for legitimate businesses of this type. They are consistent with the illicit activities the agent suspects are behind it. The agent begins to smell smoke!

Subpoenas are requested and eventually are approved and sent out. For the next couple months the agent is regularly on the phone, though often playing "phone tag" with various entities at your financial institution. The agent was trying to get copies of the transactional documentations that actually constitute potential evidence. Over that time, various subpoena compliance people kept trying to convince the agent that the simple data processing printouts they have provided is all they have to offer. The agent well knows that these are not the documents that have evidential value. The agent needs those items (or at least good copies of) created or presented during the transactions in question. What the subpoena compliance people offer may make accounting sense, but it is not the evidence the agent knows the prosecutor will want. The agent is frustrated and eventually finds you in this quest.

You do your best to be helpful but you are not sure how to get what the agent is looking for. Frankly, you are not even certain what to look for. Although you understand that what was offered were not reproductions of what happened between the teller and the customer, your training never quite covered the small nuances of teller and customer interactions. Your next concern is that the videos the agent wants are held by another department you have little contact with or control over. You already know that such videos are normally only kept for 60 to 90 days. The SAR took 45 days to find its way to the agent. The subpoena was received about a month beyond that. You believe this request will be futile. Remarkably, after repeated messages, calls and emails between the agent and that department, a couple videos of these transactions are located and preserved.

The agent presses on and becomes certain these transactional activities are also something a teller or branch employee might find memorable. Prosecutors need witnesses like this. You again feel uncomfortable because your financial institution's policy is very cautious about allowing tellers to be interviewed about official business. After another series of phone calls and email exchanges with the legal people, the interviews with the branch people are approved.

The agent interviews the teller and, as suspected, is most helpful to the agent's inquiries. These transactions are unusual and the teller recalls them very clearly. The subject has even made some unwittingly culpable statements to the teller. Not quite yet a smoking gun, but certainly not exculpatory. The agent is somewhat relieved that this live witness is available. The investigation is progressing nicely.

WHAT THE SUBPOENA COMPLIANCE PEOPLE OFFER MAY MAKE ACCOUNTING SENSE, BUT IT IS NOT THE EVIDENCE THE AGENT KNOWS THE PROSECUTOR WILL WANT

Between the analyzed financial records, the videos and the teller interviews, the agent developed the clear probable cause needed to obtain search and seizure warrants and, hopefully, to recover the extra evidence to make a stronger case. The execution of such warrants would also provide the agent with the leverage and opportunity to interview the subject under optimum circumstances.

The agent provides the prosecutor with a well-articulated, brief and concise affidavit outlining the case, and the request for the warrants. The prosecutor instinctively knows this is a competent agent and a thorough investigation. The elements and evidence for an apparent straightforward prosecution seem to be there. Although the case is already "pretty good," the prosecutor stresses to the agent that a productive interview with the subject is also going to be important.

The warrants are obtained and the agent assembles execution and search teams. The agent knows that various aspects of this enforcement plan will need to be delegated. If anything should go wrong in this plan the agent will be delegated the full responsibility of any and all failures. The agent's entire reputation and credibility will be on the line again, as it has been before. The reputation and credibility of the SAR writer will never face such a test.

Thankfully all goes well. The warrants are safely executed, valuable evidence is collected and better yet, the subject is there and makes incriminating admissions. The agent did pause a bit over the "messy" way the assisting agents conducted their searches and left the place. Not as professionally handled as hoped, but no actual damage. Although an arrest could be made, the agent knows that the subject obtaining a defense attorney is the smoother, albeit less exciting, path to closure in the case. The agent advises the subject to seek an attorney. The prosecutor is pleased.

CONFIDENTIAL AND CONGRATULATIONS DO NOT WORK AND PLAY WELL TOGETHER IN AML

Within a few days a boisterous attorney is calling the prosecutor's office professing the innocence of the client and this misunderstanding and possible miscarriage of justice. A proffer session for a formal discussion on the investigation is eventually agreed to. Of course this is "at the earliest possible opportunity," as insisted by the defense attorney.

At the proffer session, the prosecutor meticulously lays out the case. The defense lawyer becomes more quiet and deflated as all preconceived viable defense plans crumble as each piece of evidence and the elements of the crime are presented. The attorney's client was far from forthcoming during their initial consultation. The attorney now asks for indulgence and some time to speak more with the client. The prosecutor advises that a potential plea agreement will be drafted for the lawyer's review in the next couple weeks. The defense attorney no longer wants to rush things.

During the next couple of weeks, the agent fields multiple calls and requests from the prosecutor. The financial documents are repeatedly scrutinized and various clarifications, additions and corrections are requested. Additional interviews and re-interviews are requested as new questions constantly and seemingly endlessly come up. Either an outright or a perceived urgency is part of every request. Nothing is normal about the working hours associated with accomplishing these tasks. The agent and prosecutors know that the better they prepare for a trial the better chance there will not be one. The agent also knows that the prosecutor's demands may seem nonsensical at times but even the perception weakness with the case will be excessively exaggerated by the defense attorney. Each task is accomplished "forthwith."

The case becomes rock solid; the defense attorney knows that. Neither side wants a trial at this point but both threaten the consequences of that possibility until a plea is formally agreed to.

On the scheduled day of the plea, the agent, prosecutor, the accused and the defense attorney appear in court. Things are amicable between all. After about an hour before a judge explains to the defendant all the rights, nuances and procedures in the acceptance of a plea such as this, the defendant utters that magic word "guilty" to the charges.

Although the case might be considered closed, the agent cannot mark it as such until the official sentencing a couple months down the road. There are also fines, forfeitures and processing to be finalized. The agent does breathe a sigh of relief. The press release of the conviction is printed in the local paper.

While you attribute your SAR for all this, the agent attributes dog-hearted persistence in navigating all the obstacles in putting the case together. Your financial institution contributed to those obstacles. However, the agent now looks back fondly on all those frustrations. The accolades from cohorts for a successful investigation somehow always seems to do that. You, along with the agent, now could get into criminal legal trouble to even mention or seek validation that the investigation had any relationship to a SAR. Not even a double secret thank you is allowed, nor has the agent considered this as a potential oversight. Confidential and congratulations do not work and play well together in AML.

Steve Gurdak, CAMS, group supervisor, Northern Virginia Financial Initiative, Annandale, VA, USA, sgurdak@wb.hidta.org

FIXING WHAT IS NOT BROKEN:

Should you make changes to a satisfactory AML program?

An anti-money laundering (AML) program that has been deemed acceptable by regulators has reached the pinnacle and there is nowhere to go but down. So, why change anything? Changing controls in a program that has been called satisfactory is risky. Change could lead to uncontrolled risks and uncontrolled risks could lead to an unsatisfactory rating. What, then, is the impetus to make a good AML program better and why do compliance officers reevaluate or continue to monitor existing controls when those controls have been found to be effective?

The primary reason that Bank Secrecy Act (BSA) officers change otherwise static compliance programs is because the world does not stay the same. Thus, maintaining a static AML compliance program is a risk in and of itself. By changing existing controls to move an AML program forward, something better may be gained—a more comprehensive risk-rating methodology, an efficient customer due diligence process, etc. There are other, equally important, reasons to consider changing an AML program.

Changing priorities

In addition to protecting company and customer assets, a goal for any quality compliance program is to meet regulatory expectations in an efficient manner. When regulatory or cultural priorities shift, an AML program must be fungible enough to shift with the changing priorities. Take banking marijuana-related businesses (MRBs) as an example. Not long ago, providing financial services to state-sanctioned MRBs was not on any compliance officer's radar because state-sanctioned marijuana businesses were not viable under existing laws. Today, compliance officers must not only determine the risk tolerance for servicing MRBs, but also document the decision and put appropriate controls in place to support the decision.

Any financial institution that is not reevaluating its existing controls in light of the changing socioeconomic environment is taking on regulatory risk it has not even identified.

Similarly, the Fourth EU Directive[1] (4MLD) has quietly eliminated the requirement of a politically exposed person (PEP) to be foreign. According to Nina Kerkez, senior product manager at Accuity, "So far we have considered foreign PEPs, senior political, military and judicial figures as well as their families as higher risk customers when money laundering risks are looked at. With the inclusion of domestic PEPs, 4MLD also insists that enhanced due diligence is performed on these individuals by reviewing

[1] "Directive (ED) 2015/849 of the European Parliament and of the Council," *Official Journal of the European Union*, May 20, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES

their source of wealth and funds."[2] Furthermore, Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act[3] was also amended to expand the concept of PEPs to include domestic PEPs and heads of international organizations (HIOs), in addition to foreign PEPs. As a result of these changes, which came into effect on June 17, 2017, financial firms will be required to take "reasonable measures" to determine whether a customer is a domestic or foreign PEP or an HIO, or a "close associate" or family member of these types of persons. BSA officers will want to reevaluate current controls involving PEP identification and monitoring to get ahead of impending regulatory change to include domestic PEPs and/or HIO's in their programs.

Another example is the New York State Department of Financial Services (DFS) change. The DFS recently issued Part 504, Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications,[4] which became effective on January 1, 2017. The rule's beginnings lie in NY's DFS examination work, which identified problems with financial institutions' transaction monitoring and filtering systems and processes. The rule imposes governance type measures over transaction monitoring tools, ranging from periodic reviews, testing, supporting documentation for detection scenarios/thresholds, oversight and an annual board resolution tantamount to certifying compliance to the new 504 rule. The monitoring and filtering program must be based on an enterprise-wide BSA/AML risk assessment. While this is a NY state law, other states are closely watching the implementation and may intend to pass similar laws.

One final example is the renewed emphasis on reporting fraud-related money laundering offenses. With the expectation that financial institutions will be monitoring for elder financial exploitation, cybercrimes, grandparent schemes, romance schemes, lottery scams and tax return frauds, suspicious activity monitoring requirements have rapidly increased. Manual reports, automated transaction monitoring systems and investigator training must be enhanced to support the "FRAML" (fraud + AML) BSA environment. Gone are the days when an AML program could get by with monitoring solely for excessive cash or unusual international wire activity indicative of drug offenses or tax evasion.

Change in staff

The dirty little secret in the financial services industry is that AML programs operate under a budget. If they did not, the financial institution could not survive. "With the increased intensity of regulation, and the threat of fines and sanctions constantly looming over businesses, some institutions have been hindered in terms of their potential growth outside of the compliance department. Financial institutions must now attempt to find a way to optimize their efficiency and cost-effectiveness at the same time."[5] Staffing models may (and should) change when processes are made efficient; however, the BSA officer must ensure no control gaps are created as a result of staff movement or downsizing.

Change in staff that supports an institution's AML program introduces risk to a program previously deemed satisfactory. It does not need to be changes in "key positions" that lead to risk. Consider losing the person most experienced in Office of Foreign Assets Control (OFAC) sanctions in a wire transfer department.

THE DIRTY LITTLE SECRET IN THE FINANCIAL SERVICES INDUSTRY IS THAT AML PROGRAMS OPERATE UNDER A BUDGET

[2] Nina Kerkez, "Fourth Anti-Money Laundering Directive—How does it affect you?," Accuity, March 21, 2016, https://accuity.com/accuity-insights-blog/4th-money-laundering-directive-how-does-it-affect-you/

[3] "Politically Exposed Persons and Heads of International Organizations—Life Insurance Companies, Brokers and Agents," FINTRAC, June 2017, http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide15/15-eng.asp

[4] "Part 504," Department of Financial Services, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf

[5] Christopher J. Pelaez, "AML Compliance Costs—How much is enough?," Global Radar, August 25, 2016, https://www.globalradar.com/aml-compliance-costs-how-much-is-enough/

The BSA officer must ensure the existing controls are comprehensive enough to sustain the program in light of the loss of the person with expertise.

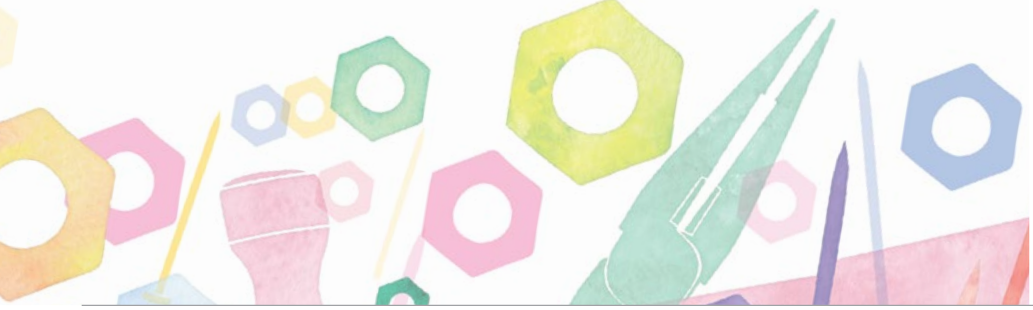
Change in leadership

An incoming experienced BSA officer will also, undoubtedly, reevaluate existing controls in a satisfactory program. The skilled BSA officer brings with him/her knowledge gained from prior examinations and information gained from networking and industry training along with a keen understanding of risk-based controls. A new set of eyes on a successful program may highlight potential risks not previously identified. With the current emphasis on personal liability, a BSA officer taking leadership over an existing program must have complete understanding and faith that the existing controls adequately cover identified risks and that residual risk falls within the risk tolerance for the organization. NY DFS Part 504 essentially requires a BSA officer new to an organization to very quickly comprehend the program and systems and have faith in those same programs and systems to put their reputations and personal finances on the line.

Mergers and acquisitions

A significant change in the size, geographic footprint, product offering and/or customer base due to a merger or acquisition should result in a reevaluation of current controls. "Identify the specific risk categories (i.e., products, services, customers, entities, transactions and geographic locations) unique to the bank"[6] is the recommended first step to a comprehensive risk assessment as outlined in the Federal Financial Institutions Examination Council's BSA/AML Examination Manual. Knowledge of the specific AML risks posed by a merger or acquisition is a critical step in performing a gap analysis. The BSA officer will map the current controls to any newly identified risk to identify gaps in the program. The BSA officer will then determine if the gap is acceptable or must be mitigated with new or enhanced controls. Failure to reevaluate the control in light of risks from a merger or acquisition leaves the financial institution open for regulatory criticism.

THE ART OF BEING A BSA OFFICER IS THE ABILITY TO BALANCE THE NEED FOR TECHNOLOGICAL CHANGE IN A PROGRAM, THE DESIRE TO REAP THE BENEFITS OF IMPROVED TECHNOLOGY AND THE COST OF IMPLEMENTING AND MAINTAINING ADVANCED TECHNOLOGY



Change in technology

The pace of technological change has accelerated in the last two decades. AML programs are not immune from advancing technology. In addition, "with the rise of regulatory practices becoming strictly enforced at both the national and international level, financial institutions are faced with the fact that AML software that was once viewed as an unnecessary luxury for the company has shifted to an essential component in everyday operations."[7] The art of being a BSA officer is the ability to balance the need for technological change in a program, the desire to reap the benefits of improved technology and the cost of implementing and maintaining advanced technology. It becomes easy to justify the need for new or improved technology when an examiner points out deficiencies in an AML program. When an AML program is operating effectively, separating the need for enhanced technology from the desire to have enhanced technology becomes much more difficult.

In theory, improved technology equals better controls. Enhanced screening capability should translate to fewer false positives or fewer missed positives, which should result in more focused reviews. Advanced monitoring capability should

[6] "Bank Secrecy Act/Anti-Money Laundering Examination Manual," FFIEC, 2014, https://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2014.pdf

[7] Christopher J. Pelaez, "AML Compliance Costs—How much is enough?," Global Radar, August 25, 2016, https://www.globalradar.com/aml-compliance-costs-how-much-is-enough/

equate to an increased alert to SAR ratio. The operative word in the prior scenarios is "should." Oftentimes changing technology opens an AML program to increased risks from incorrect or incomplete data ingestion. Optimal tuning is critical to achieving desired output. In addition, to minimize the risk of regulatory scrutiny, all decisions and rationale regarding changing technology must be well-documented. "With the vast amounts of information available to decision-makers, 'gut feel' business decisions are not sufficient to satisfy internal auditors or examiners.

Decisions must be supported with well-documented rationale and evidence and tracked to evaluate whether assumptions hold true initially and over time."[8]

That being said, there are certainly times when a financial institution with a solid AML program should consider investing in improved technology for the AML program such as when there is potential for an acquisition or the technology comes with additional controls (e.g., systemic checks of the required fields in suspicious activity reports or currency transaction reports to reduce errors).

Industry-led change

Enforcement actions

Enforcement actions can be change agents. They are public documents available for study by BSA officers. Fines for program failures have increased over the last several years as has the reach of FinCEN's enforcement activity. Financial institutions, casinos, MSBs and even a precious metals dealer have felt the effect of these actions. The content of enforcement actions can be a rich learning ground for BSA officers who may use them to modify their already satisfactory AML programs.

A STATIC PROGRAM IS
A PROGRAM AT RISK

ACAMS initiatives

ACAMS and other trade and industry groups can influence change through their initiatives, classes and products that they offer. For example, some BSA officers have adopted the ACAMS risk assessment tool to use to create their risk assessments. Others have attended ACAMS conferences and learning events where they hear of tips and tricks of the trade, which becomes the impetus for change.

Industry best practices

Some contemplate changes to AML programs based on industry best practices. Take FinCEN's new customer due diligence/beneficial ownership rule for which compliance is required by May 11, 2018. BSA officers are talking to each other and developing best practices surrounding the rule. As a specific example, although not required, some banks have included information on their websites to prepare their prospective customers for the ownership questions they may get starting on May 11.

Changes in regulation/ regulatory scrutiny

While obvious, we would be remiss if we did not point out a critical reason for changing an AML program and that is changes to the statute and/or other regulatory guidance. The aforementioned customer due diligence/beneficial ownership rule is a perfect example of a reason to change an AML program. FinCEN advisories, OFAC sanctions programs updates and special measures are also all reasons for BSA officers to consider changing their BSA compliance program.

In addition to specific changes to the BSA, just in general, BSA/AML regulations receive seemingly constant scrutiny from a plethora of regulatory bodies. Some reviewers question whether BSA/AML is working to prevent money laundering; others believe BSA compliance to be burdensome—particularly so on smaller organizations.

No matter the reason for the review, it is important for BSA officers to be aware of the reviews should they influence change on the current regulation.

Conclusion

The reasons to change a satisfactory AML program run the gamut and are important considerations for BSA officers. The risk of maintaining the status quo is that additional or other risks will have presented themselves since the program was evaluated. A static program is a program at risk. To paraphrase a quote from an unknown author: BSA officers must not be afraid of change—good controls may be eliminated, but better controls may be gained.

Amy Wotapka, CAMS, BSA officer, First American Bank, Vernon Hills, IL, USA, awotapka@firstambank.com

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

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

[8] "AML Model Risk Management and Validation," EY, 2013, http://www.ey.com/Publication/vwLUAssets/EY_-_AML_model_risk_management_and_validation/$FILE/EY-AML_model_risk_management_and_validation.pdf

CAREER GUIDANCE

Attracting compliance talent

For financial institutions around the world, attracting and retaining top talent in the compliance team is essential. As regulatory scrutiny has ramped up in recent years and the focus on preventing financial crime and terrorist financing has intensified, the need for banks to employ skilled compliance professionals has become more pressing than ever before.

However, in a competitive market the top compliance talent can be hard to come by. Research published last month by SWIFT, Dow Jones and ACAMS found that having enough properly trained anti-money laundering (AML) staff was a concern for 57 percent of the AML professionals surveyed—up from 36 percent in 2013—and 26 percent of respondents listed this as their top challenge.[1] Therefore, banks are having to work harder than ever before to attract confirmed compliance talent from other banks and vendors. At the same time, banks are proactively developing in-house talent to meet their compliance needs.

Against this backdrop, it is important to take all measures necessary to attract, retain and develop top compliance talent. One way in which banks can achieve this is by building a strong compliance culture across the organization.

Why choose compliance?

In the past, the compliance function has not always been seen as the most attractive career opportunity by ambitious candidates. There is a lingering perception that compliance, while necessary to the organization, acts as a hindrance to business development. As such, some talented candidates have preferred to focus their attention on business development opportunities.

However, while today's more stringent regulatory environment is not without its challenges, it has also highlighted the considerable appeal of a career in compliance. For one thing, compliance is increasingly seen as a noble cause, which speaks to the values of many professionals. Working to prevent the illicit money flows that support terrorist financing, human trafficking, drug dealing and corruption means that people working in this area feel they are making a positive contribution to society and building a better world.

At the same time, compliance is an intellectually demanding discipline, presenting challenges that are likely to appeal to high achievers. Not all compliance roles are the same, but whether an individual is a specialist compliance expert or a general management professional supporting the compliance team, the role of the compliance professional is both challenging and fulfilling.

There is much that will draw top talent to a career in compliance, but in a competitive recruitment climate banks cannot rely on this appeal alone. By tapping into opportunities for innovation and collaboration in this area, banks can build a culture of compliance that will not only achieve cost and efficiency benefits, but also increase the appeal of their organizations for compliance professionals.

Innovation

Central to building a compliance culture is the adoption of innovative technology. While the prospect of having to comply with regulations may not be appealing in and of itself, organizations that position compliance as an epicenter of innovation and actively pursue new opportunities to drive efficiency, have more to offer candidates than organizations that approach compliance as a tick-box exercise.

There are a number of ways in which compliance professionals can embrace innovation. In order to achieve compliance with the necessary regulations, professionals need to make sure that their processes and policies are effective, and that they meet expectations. With this achieved, compliance staff can then explore innovations that can increase the efficiency of the organization in meeting regulatory requirements. Beyond this, specific regulations may present opportunities for financial institutions to achieve further improvements.

Leveraging the DFS regulation

Last year's publication of the New York Department of Financial Service's new risk-based anti-terrorism and anti-money laundering regulation is an example of how banks can take advantage of regulations in order to achieve further advancements. The regulation requires banks operating in New York to maintain appropriate watchlist filtering and transaction monitoring programs. Banks are also required to carry out regular testing and demonstrate that their programs are both compliant and aligned with the organization's risk appetite.

Institutions affected by this regulation can simply choose to fulfill the requirements. Alternatively, they can take advantage of the opportunity that the regulation presents to enhance their quality assurance programs and to build a more robust compliance regime, thereby reducing costs and improving the efficiency of their environments.

Embracing continuous improvement

The same is true of other regulatory requirements. Throughout the compliance discipline, there are opportunities to embrace innovation and to adopt a mindset of continuous improvement.

For example, sanctions screening involves checking transactions for names that appear on regulators' sanctions lists. To achieve this, banks have to refine the parameters of their sanctions screening filters to make sure that they identify illicit transactions, even if names do not appear exactly as they do on the sanctions list.

[1] "2017 Global Anti-Money Laundering Survey," Dow Jones and SWIFT, http://go.dowjones.com/AMLsurvey2017

Inevitably, this will generate many false positives. Banks can address this by adopting a continuous improvement mindset in order to increase the efficiency of their systems without compromising their effectiveness. This approach can reduce costs, thereby benefiting the organization as a whole while also making compliance roles more attractive to potential candidates.

Adopting new technologies

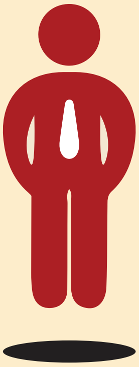
By the same token, talented professionals will be attracted by opportunities to take advantage of new and emerging technologies. As banks work to improve the effectiveness and efficiency of their processes, they are exploring the use of artificial intelligence, robotics and machine learning to tackle financial crime. For instance, in the area of sanctions screening, banks might use robotics to identify and close false positives automatically by sourcing information that proves an alert is not relevant.

Where talent is concerned, being exposed to cutting-edge technologies is an attractive part of the job. Many of these developments are being driven by Fintech and Regtech companies, providing an interesting learning experience for compliance professionals. Such developments also free up people's time, enabling them to focus their intellectual powers on the cases that need the most advanced analysis, rather than spending time on false positives that can easily be dismissed with supplementary information.

"Easier access to information means that compliance professionals won't have to spend their days chasing customers or filling out forms, removing an element of repetition and 'grinding' from the job," comments Mark Brotherton, director of fraud and financial crime at Lloyds Bank Commercial Banking. "Instead, these workers will be able to focus their energy on tasks that require more critical thinking, such as building relationships and educating customers and banking partners. Plus, more interesting work helps to attract young talent and to retain high performing staff."

Collaboration

The focus on innovation makes compliance an exciting place to be, but beyond this, the collaborative nature of the job provides further opportunities for professionals to grow their networks while enhancing their skills and reputation.



WHERE TALENT IS CONCERNED, BEING EXPOSED TO CUTTING-EDGE TECHNOLOGIES IS AN ATTRACTIVE PART OF THE JOB

For one thing, internal collaboration is an important part of the job. In order to achieve the necessary level of compliance, professionals working in this area need to engage with colleagues across all divisions of the organization, from operations to sales.

Rather than imposing requirements on their colleagues, compliance professionals will need to develop interpersonal skills in order to secure their cooperation.

Furthermore, compliance professionals have the opportunity to interact extensively with their peers across the industry. Financial crime compliance is a non-competitive area: financial institutions do not as a rule win market share by being more compliant than their competitors. As such, banks are generally willing to talk to each other and share information to the extent possible within privacy constraints. Compliance utilities are being developed to facilitate information sharing, drive process standardization and increase transparency across the industry.

That said, banks' ability and willingness to share information can vary depending on their geographical footprints. While some countries have a national framework in place allowing for this type of information exchange, less is available at the international level. At the same time, large banks may find it more difficult to share information given the complexity of their legal structures, the broader geographical spread of their activities and the complexity of their legal environments.

Nevertheless, many banks are willing to participate in information sharing in the interests of increasing effectiveness and efficiency across the industry. Industry working groups and forums may provide an opportunity to achieve this, while public/private partnerships are taking this to the next level. Examples include the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia's financial intelligence agency which works in partnership with industry and government agencies. Meanwhile, in the U.K., the Joint Money Laundering Intelligence Taskforce (JMLIT) was set up in 2015 to improve intelligence sharing arrangements and to combat high-end money laundering.

By sharing practices, innovation and ideas in this way, compliance professionals can help to tackle financial crime at an industry level. They can also benchmark their institutions against others in the industry in order to identify opportunities for improvement.

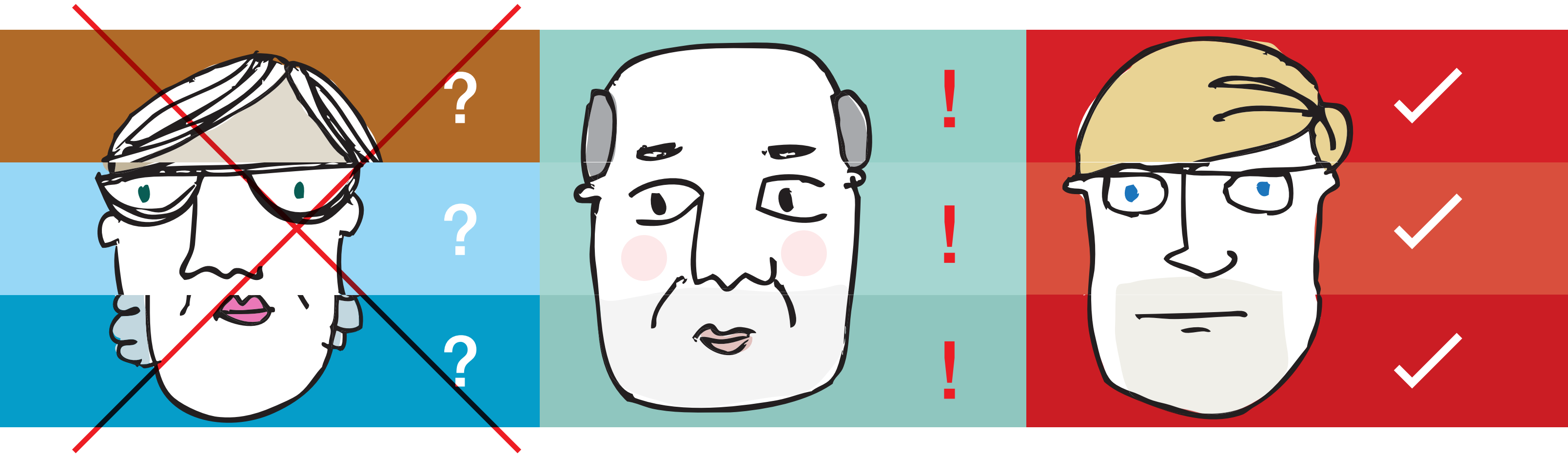
Conclusion

In the current market, financial institutions have much to gain by developing a strong compliance culture. As well as mitigating risks and generating cost savings and efficiencies, institutions can also position themselves to attract top compliance talent in an increasingly competitive recruitment market.

Rather than simply focusing on meeting requirements, the individuals who work within a strong compliance culture can enjoy fulfilling and challenging careers. As well as the satisfaction of contributing to the industry-wide fight against financial crime, compliance professionals can leverage cutting-edge technology to drive efficiency within their own organizations. Furthermore, they have the opportunity to build strong networks both within the organization and beyond—potentially contributing to collaborative initiatives that can improve standards and practices across the industry.

Luc Meurant, head of financial crime compliance services, SWIFT, Brussels, Belgium

Name Screening / there are **3 things** a system must do brilliantly



1 The **filter** must flag genuine hits while minimising mismatches.

People may easily understand where two rather different spellings of a name represent the same person. A good filter will combine such fuzzy detection capabilities with the ability to tune to an organisation's characteristics, minimising mismatches.

2 **The lists** must be standardised, cleansed and maintained rigorously.

Sanctions lists are notoriously inconsistent and dynamic in their structure and level of detail. SWIFT standardises and cleanses the data to optimise screening effectiveness and reduce false positives. Updates are automatic, so you never have to worry about outdated information.

3 The system must go through ongoing **quality assurance** to ensure it

In the real world, name presentation may change or names may simply be mistyped. Equally, lists are constantly updated. SWIFT's Name Screening service undergoes regular and exhaustive testing, maintainence and optimisation.

And we added a 4th …simplicity

SWIFT's new **Name Screening** service provides powerful technology, list management, and quality assurance, all with the simplicity of a secure hosted solution. Fully managed by SWIFT, it enables you to screen entire databases and check individual names using an online service built and managed for the industry, by industry experts to world-class standards.

To find out more visit
www.swift.com/namescreening

SWIFT

Lauren Kohr and Jack Sonnenschein:

Obtaining a 'world-class' certification

Lauren Kohr

Jack Sonnenschein

A*CAMS Today* had the opportunity to sit down with two graduates of the Advanced Certification program, which aims to provide financial crime professionals with the tools and knowledge to elevate their careers and skillset to a top-tier level. The program consists of a three-day live program of lectures, discussions and group exercises, and the contribution of a white paper on an approved topic.

ACAMS Today spoke with Lauren Kohr, CAMS-FCI, risk officer at Old Dominion National Bank, and Jack Sonnenschein, CAMS-Audit, founder and principal of Compliance Navigation LLC, about their experiences with the Advanced Certification program and how it helps their careers.

***ACAMS Today:** What prompted you to pursue your Advanced Certification?*

Lauren Kohr: My passion resides in combating financial crimes. CAMS-FCI provides a framework to develop the skills and expertise to identify and unveil complex financial crimes. Having my passion intersect with an opportunity to advance my knowledge prompted me to pursue the opportunity. The result was an elite certification that aligned with my professional interests and goals.

Jack Sonnenschein: There's a saying, "If you're not moving forward, you're falling behind!" AML is dynamic and constantly changing. Getting an Advanced Certification demonstrated my desire to keep moving forward.

AT: *Has the Advanced Certification helped you advance in your career and/or in your day-to-day tasks? If so, how?*

LK: The ACAMS Advanced Certification is seen as a world-class certification in the industry. It has provided me increased credibility with regulators and industry professionals. Several opportunities that have complimented by career continue to transpire based on the white paper I authored and professional relationships that were fostered during the live program. From a day-to-day perspective, the knowledge and skills obtained from the certification led me to enhance our AML program through new typologies geared toward complex financial crimes, increased investigation standards and effective suspicious activity reporting. The enhanced program has been praised by our community bank examiners, and law enforcement has praised the quality and content of the suspicious activity report narratives written by my team.

JS: The Advanced Certification sends a message loud and clear about how seriously I take my profession and how committed I am to advancement. Career-wise, it sets me apart.

AT: ***As part of the Advanced Certification process, you are required to author a white paper. How did you choose your topic?***

LK: After attending an industry event, I walked away inspired to author a paper that would provide concrete solutions to a challenge currently faced by AML and Bank Secrecy Act (BSA) professionals. At the time, legalization of marijuana at the state level was in its infancy stages and regulatory guidance had just been issued. I knew, regardless of a financial institution's position on banking marijuana-related business, it would impact their BSA/AML program. By choosing a topic and writing a white paper related to the challenges of banking the marijuana industry, it provided an opportunity to expand my knowledge of the emerging industry and assess the risks and impact to a financial institution's BSA/AML program. It also helped me identify typologies and it provided an effective approach to addressing the challenges and risks.

JS: Choosing a topic was easy! I just went with my passion: training and helping others develop and implement the independent testing pillar of BSA/AML programs. When it comes to terrorist financing and human trafficking, it's essential that people are well trained.

> I JUST WENT WITH MY PASSION: TRAINING AND HELPING OTHERS DEVELOP AND IMPLEMENT THE INDEPENDENT TESTING PILLAR OF BSA/AML PROGRAMS
>
> —JACK SONNENSCHEIN

AT: ***Once the topic was chosen, what were the next steps? What kinds of research tools helped you in the process?***

LK: Once I settled on a topic, thought about and outlined the objectives, main message, current challenges, proposed solutions, and takeaways, I was easily able to supplement my content with open-source research, regulatory guidance, and apply my personal industry knowledge and experience. I was successful in conducting personal interviews and utilizing my network of industry subject-matter experts for opinions and recommendations. My ACAMS mentor was also a good source for guidance and recommendations on research tools and approaches as well.

JS: There were plenty of enforcement actions that referenced deficiencies in staff training. In particular, they cited independent testing personnel as not having the requisite skills and expertise to do their work. The next step was to consider the root causes of the problems and how to address corrective actions on a sustainable basis. It wasn't easy, but it did seem to flow pretty smoothly once "pen went to paper," so to speak.

AT: ***What advice can you give to members looking to obtain an ADV certification?***

LK:

- **A**spire to achieve a certification that can change the course of your career, set you apart from your peers, deepen your knowledge and show you desire to grow yourself and your career.
- **D**evote the time needed to self-study, prepare for the live program and write an impactful white paper that represents your expertise as an advanced practitioner.
- **V**enture beyond your comfort zone during the live program. Meet, network and develop professional relationships with the instructors and attendees.

> ASPIRE TO ACHIEVE A CERTIFICATION THAT CAN CHANGE THE COURSE OF YOUR CAREER, SET YOU APART FROM YOUR PEERS, DEEPEN YOUR KNOWLEDGE AND SHOW YOU DESIRE TO GROW YOURSELF AND YOUR CAREER
>
> —LAUREN KOHR

- **I**nvest yourself fully in the entire program. As a participant, you have been awarded a unique opportunity to learn, network and align with the industry's best instructors and other passionate professionals.
- **C**hallenge yourself to write your white paper on a topic you and other AML professionals would strongly benefit from having as a resource.
- **E**nroll yourself now into the program. It was one of the best investments I have made in my career. Not only has it helped me reach new professional heights, but I have also gained the knowledge, expertise and skills needed to identify, investigate and properly report on complex financial crimes.

JS: Taking a line from Nike, "Just do it." There will never be a shortage of reasons not to do it, and that's what sets people apart from the rest—achieving the certification.

Interviewed by: Larissa Bernardes, web editor, ACAMS moneylaundering.com, Miami, FL, USA, lbernardes@acams.org

CARROTS AND STICKS... AND SANCTIONS

From behind a bank of computer monitors, performing day-to-day compliance operations, it is easy to see economic sanctions as a binary thing: sanctions targets are *persona non grata*, and everyone else is not. However, from a policy level, sanctions are a much more multifaceted tool of statecraft that provides great flexibility in both exerting pressure and minimizing the impact on one's own economy.

Who is sanctioned?

The first area where regulators can show flexibility is in the designation process. Designations are generally very specific, although the Office of Foreign Assets Control (OFAC) 50 Percent Rule (and its equivalents elsewhere in the world) significantly expands the reach to parties related to those designated. On the other hand, the wording of regulation or government order (e.g., Executive Orders in the U.S.) make whole classes of people subject to sanctions as long as there is knowledge that a person or entity meets the definition of those subject to sanctions. Those documents typically cover specific ranges of actions taken in the past (e.g., participation in the assassination of Lebanese officials) or on an ongoing basis (e.g., contributing to the instability in a country). Typically, they also contain clauses that cover assistance to those participating in the specified activities, as well as provision of financial or technical support to them. In addition, a number of sanctions programs target specific exports or even entire industries in the sanctioned country.

Choosing to add listings to a sanctions program, or refraining from doing so, permits the sanctioning country to balance the relative amounts of "stick" (i.e., amount of pain in conducting financial affairs) and "carrot" (i.e., providing incentive to change behavior so that sanctions could be loosened at a future date). And this is not merely a theoretical bargaining chip. For example, the U.S. chose not to add names to the Myanmar sanctions program, despite recommendations from the State Department to do so, because it was conducting negotiations in secret with the ruling junta on democratization of that society.

What is sanctioned?

The next thing to determine is what sort of restrictions apply. There is more variation than one might expect.

The bulk of economic sanctions imposed on specific targets are "do not do business" type of prohibitions. However, even here there are two very different types of sanctions, each associated with a different goal of sanctions. The most common sanctions are asset freezing or blocking sanctions, where the assets associated with an account or transaction are made unavailable to all parties (i.e., both the account holder/transactor and any counterparty). Such sanctions are intended to prevent the use of assets by seizing them. In contrast, certain sanctions result in funds being returned to the party wishing to effect a transaction. In these cases, assets can be utilized for the intended purpose—just not in the sanctioning country's financial systems or broader economy. As appropriate examples, the U.S. imposes a number of these sorts of sanctions, including the sectoral sanctions imposed on Russian energy, defense and financial services firms (as does the EU), and for example, the parties on OFAC's Non-SDN Palestinian Leadership Council (NS-PLC) List (part of the Consolidated Sanctions List). While there is certainly inconvenience in such sanctions, the desired business can still be conducted elsewhere, perhaps at greater cost. If such restrictions are imposed unilaterally by a country rather than by a larger, more global coalition of nations, their effect is more of a slap on the wrist than an effort to inflict true economic hardship. Thus, while NS-PLC restrictions are largely symbolic, the sectoral sanctions, which were also adopted in the EU, have a significant impact on the designated sectors of the Russian economy.

Generally, a sanctions designation prevents all manner of transactions involving the targeted individual or company (or cargo vessel or aircraft, in OFAC's case).

THE BULK OF ECONOMIC SANCTIONS IMPOSED ON SPECIFIC TARGETS ARE "DO NOT DO BUSINESS" TYPE OF PROHIBITIONS

However, sanctions can be restricted to specific classes of transactions. This allows the impact of the restrictions to be more finely calibrated—both the impact on the sanctions target and the consequences of those sanctions on the customers, suppliers and business partners of the target. The sectoral sanctions imposed on elements of the Russian economy is an apt example. These sanctions only prohibit dealing in long-term capital market issues and specific types of energy exploration activities. By doing so, Russian energy firms can continue to perform their current business activities but—because the sanctions impede the raising of capital via the securities markets—they will face challenges trying to finance the expansion of their business. In addition, even if they could continue to perform, they would be unable to obtain outside technical or other assistance in the actual exploration activities due to the prohibitions of OFAC's Executive Order 13662 Directive 4 and its EU equivalent. However, by not actually sanctioning all business with these firms, while these firms' strategic planning for their business will be impacted, they will still be able to sell their current set of goods to Western Europe, which relies on their products. Had the sanctions been more comprehensive, Europeans might have struggled to meet their energy needs.

Beyond these financial sanctions—which largely (with the exception of the aforementioned energy exploration restrictions) revolve around restricting the flow of financial assets—once a sanctions program expands to encompass a country's economy and not merely specific citizens, an even broader spectrum of economic sanctions can also be applied.

Perhaps the most notable of these restrictions are sector-specific or blanket restrictions on international trade, as well as transactions using the sanctioned country's cargo vessels. An adjunct to these prohibitions is the one usually imposed on actions that facilitate third-party transactions. These include provision of approvals or guarantees, financial transactions such as financing or insurance related to the transactions, as well as any services that help advance the transaction, such as providing advisory services. In addition, investments in a country's economy are also typically prohibited.

Broad prohibitions, of course, permit an almost infinite level of discretion when it comes to the actual breadth of those restrictions. For example, when Myanmar had broad sanctions imposed on them, the import restrictions were limited to Burmese jade, jadeite and other precious stones. Similarly, U.S. Iranian import prohibitions currently have a carve-out for carpets and foodstuffs—although that exception was terminated for a period of time when maximum pressure was being applied to Tehran. In addition, there was a significant liberalization of a number of OFAC Cuba sanctions prohibitions during the latter stages of the Obama presidency. Such measured adjustments to sanctions programs provide shows of goodwill, while providing some modicum of economic relief as an incentive for continued good faith dealings.

Secondary sanctions: The long arm of sanctions law

Secondary sanctions provide a mechanism by which regulators can exert pressure on foreign persons and companies whose actions make the domestic sanctions less effective in achieving their goals. These sanctions are used when the regulator does not have jurisdiction to impose the types of consequences (such as civil monetary penalties) that can be levied on domestic persons and firms. While relatively new as a compliance term, secondary sanctions are not really all that new as a policy tool. One can consider the use of the Entity List by the Commerce Department's Bureau of Industry and Security, as well as the Section 311 sanctions imposed by the Financial Crimes Enforcement Network as the imposition of secondary sanctions, as two prominent examples that fit the functional definition, but with which one may not associate the term "secondary sanctions."

While being placed on the Entity List is pretty cut and dried (exports to firms on the list require licenses), the other programs all present a range of options. The Section 311 sanctions options (called Special Measures) include:

- Enhanced reporting and record keeping requirements for correspondent accounts
- Required acquisition of beneficial ownership information for the account subject to the Special Measure
- Required identification of and information gathering for each customer using correspondent or payable through accounts (PTAs)
- Outright bans on opening or maintaining correspondent accounts

In contrast, the Part 561 secondary sanctions options (part of OFAC's Iranian sanctions program) can result in one or more of the following restrictions being imposed, in lieu of outright denial of correspondent relationships:

- Restrictions or prohibitions on trade finance transactions
- Restrictions or prohibitions on foreign exchange transactions
- Restrictions on transaction types
- Limits on the number of and/or monetary value of transactions
- Requiring pre-approval of each transaction

And while the Non-SDN Iran Sanctions Act List (NS-ISA) is currently empty, due to the changes wrought by the Joint Comprehensive Plan of Action (JCPOA), the Act provides for the imposition of five or more of the following restrictions:

- Prohibition on assistance from the Export-Import Bank for exports to the sanctioned subject
- Restrictions on loans from U.S. banks
- Prohibition on being a primary dealer in U.S. government securities
- Prohibition on holding U.S. government funds on deposit
- Prohibition on procurement from the sanctioned party
- Prohibition on foreign exchange transactions
- Prohibition on all banking transactions
- Prohibition on ownership of any U.S. property
- A requirement to obtain export licenses for all controlled goods exports to the sanctions target
- Prohibition on investing in securities issued by the sanctioned party
- Travel restrictions on the firm's officers

Each of these possible regulatory actions imposes a commercial penalty on the target of that action. While, to date, those designated under these programs have largely been given the maximum possible penalty, the way regulations are written provides a significant amount of flexibility to regulators. As behavior changes, the level of ongoing restriction on business dealings can be adjusted up or down to provide incentives for continued compliance with regulatory expectations or disincentives for continued non-compliance.

SECONDARY SANCTIONS PROVIDE A MECHANISM BY WHICH REGULATORS CAN EXERT PRESSURE ON FOREIGN PERSONS AND COMPANIES WHOSE ACTIONS MAKE THE DOMESTIC SANCTIONS LESS EFFECTIVE IN ACHIEVING THEIR GOALS

Exceptions to the rules

It is generally easier to prohibit a wide swath of behavior and to determine the exceptions, than it is to be more granular in specifying what is banned, unless the sanctioned activities are very narrow in scope. Recent history has shown that, sometimes, the seemingly narrowest of prohibitions today can lead to the realization that exceptions are still warranted tomorrow. Consider that one of the first General Licenses imposed under the Ukraine-related OFAC sanctions was to permit business with the Turkish bank DenizBank, which was wholly-owned by Sberbank and thus subject (due to the "50 Percent Rule") to the same sanctions as its parent. Recently, after the Russian Federal Security Service (known in the West as the FSB) was designated under OFAC's cyber sanctions. A General License was quickly issued to permit payment of fees to the FSB for forms processing that they perform on a routine basis.

ONE MORE WAY THAT REGULATORS CAN SHOW FLEXIBILITY IS THROUGH GUIDANCE DOCUMENTS, SUCH AS STATEMENTS OF LICENSING POLICY

Even General Licenses are not uniform in their operation. Some are time-limited (and often get extended); licenses for dealings with companies in Belarus and firms associated with Panamanian firms owned or controlled by Specially Designated Narcotics Trafficking Kingpins are the most prominent of this type. Others have reporting requirements, which increase the burden (and, therefore, the desirability) of maintaining those business ties. Most notably, the ability as part of the Trade Sanctions Reform and Export Enhancement Act to export certain foodstuffs, medicine and medical supplies to certain sanctioned countries is not a blanket authorization, but requires an exporter to obtain a one-year specific license for these activities. In fact, in 2016, multiple divisions of Alcon received a civil monetary penalty from OFAC for not obtaining that license on a consistent basis.

These additional sanctions program elements serve a number of useful purposes. Reporting and explicit licensing requirements permits a level of control and transparency regarding the limited flow of assets under these programs. They help curtail abuse of the exceptions (which is why these licensing elements are largely only imposed on countries that are comprehensively sanctioned), and raise the stakes for those looking to skirt the sanctions regulations in that way.

One more way that regulators can show flexibility is through guidance documents, such as statements of licensing policy. These provide guidance as to what exceptions to sanctions prohibitions will generally be approved for a specific license.

For example, the Statement of Licensing Policy for export or re-export of commercial passenger planes, and related parts and services states, in part that "the following Statement of Licensing Policy establishes a favorable licensing policy under which U.S. and non-U.S. persons may request specific authorization from OFAC to engage in transactions for the sale of commercial passenger aircraft and related parts and services to Iran." It then notes that the aircraft being sold must be used exclusively for civil aviation, and that authorized services would include "warranty, maintenance, and repair services and safety-related inspections" for the aircraft used exclusively for commercial passenger flights. Such statements are intended to make companies less wary in engaging in specific transactions by clearly stating which applications are likely to be approved. The availability and breadth of such guidance is an additional tool to provide incentives or disincentives for continued compliance with sanctions program objectives.

A thick rule book

Having to deal with the granular nature of sanctions regulations and the exceptions to those somewhat general rules adds considerable time and effort to sanctions compliance efforts. In earlier days, when the U.S. only had blanket sanctions on North Korea, Cuba and North Vietnam, compliance processing was easier to complete in less time with fewer people needed for a proper review of potential violations. However, it came with regulators' inability to offer intermediate steps between a blanket set of prohibitions and none at all.

In contrast, now is an emergent golden age for finely tuned regulatory carrots and sticks to more optimally achieve foreign policy goals. The only downside is that someone has to pay the bill for the shiny new toys. And, once again, it is the private sector that is stuck with the check, paid every day in extra staff, more involved policies and procedures, more extensive and complex training, and more rigorous program testing.

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

The ultimate BENEFICIAL OWNERSHIP IDENTIFICATION REQUIREMENT:

WHY IT MATTERS TO ALL OF US

Money laundering, terrorist financing, evading taxes, bribery, corruption, abuse of human rights and even modern-day slavery differ in their nature, but they have some things in common: They destroy people's lives, undermine the common values in our societies and they are facilitated by a lack of transparency.

Global money laundering transactions are estimated at 2 to 5 percent of global GDP.[1] The cost of corruption equals more than 5 percent of global GDP, with over $1 trillion paid in bribes each year.[2] More than $12 trillion has been siphoned out of Russia, China and other emerging economies into the secretive world of offshore finance.[3] Criminals hide behind a veil of complex and anonymous corporate structures, funneling dirty money into the legitimate financial market, evading taxes and enjoying the proceeds of crime, yet remaining untraceable to law enforcement agencies.

Anyone with experience in the compliance field will be familiar with these facts. There is no shortage of data that illustrate the scale and cost of the problem. The Financial Action Task Force's (FATF) 40 Recommendations published in 2004 addressed the connection between business secrecy and financial crime. The World Bank's Stolen Asset Recovery report of 2011 ("The Puppet Masters") showed that of 150 corruption cases worth over $50 billion in illicit assets, nearly all involved the use of the companies with concealed ownership. But to your friends and family, the 2016 media blast around Panama Papers may have come as a revelation. It may have been the first time most civil society realized what the compliance world had known for decades. Such discoveries of the scale and pervasiveness of financial crime are needed for society to demand the changes necessary to effectively fight financial crime. As members of society, we can demand change from our political representatives for better regulations and their enforcement.

As part of the compliance environment, it is our duty to the rest of society to help prevent all forms of financial crimes. Thus, the requirement to uncover the true persons behind legal entities is key. However, the prevailing secrecy in corporate vehicles makes it often an impossible task for financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) to comply with anti-money laundering (AML) and anti-bribery and corruption (ABC) regulations and effectively identify the beneficiaries of legal entities.

Who is the UBO?

There is no universal definition of "beneficial owner." Various bodies, governments and institutions differ in their interpretations. FATF, which sets the global standards in money laundering efforts, defines a beneficial owner as "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement."[4] With regards to the owning threshold, FATF does not provide a clear answer and only provides 25 percent as an example.

How civil society can drive the change

With numerous large-scale corruption and tax avoidance scandals reaching the mainstream media every month, civil society is now more than ever aware of how the lack of transparency in corporate structures can have a negative effect on the economy and how, through anonymous entities, stolen assets can be transformed into luxurious villas, private jets and fast cars. Increased engagement against business secrecy from charities and non-profit organizations, but also journalists' groups working against corruption, has helped to build momentum. For example, a special report by *Reuters* in 2012 highlighted how one high street coffee shop chain avoided paying taxes on profits in the U.K. through a complex corporate structure. This led to a widespread media debate and in turn to customers boycotting the chain. Not only did the action have an enormous negative impact on the company's reputation, but it also forced it to make changes to its tax maximization practice in the U.K.[5]

Abuse of the housing market

Various organizations, including Transparency International, Global Witness, Tax Justice Network and ClampK, have been leading successful campaigns to reveal the misuse of corporate vehicles and the funneling of "dirty money" into the U.K. housing market. Abuse of the market directly impacts property prices in the country's capital, making housing unaffordable to the working class. The U.K.'s National Crime Agency reported that as much as 100 billion pounds in tainted cash passes through the U.K. each year, with significant sums invested in London's thriving high-end housing market.[6] The civil society's pressure has had a definite influence on the delivery of the government's commitment to introduce the updates into the Criminal Finances Bill. The new regulation

[1] The International Monetary Fund, http://www.imf.org/external/index.htm

[2] World Economic Forum, https://www.weforum.org/

[3] Tax Justice Network, https://www.taxjustice.net/

[4] "Transparency and Beneficial Ownership," FATF Guidance, October 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf

[5] Sylwia Wolos, "Business Transparency in the Fight Against Financial Crime," Thomson Reuters, December 2, 2015, https://blogs.thomsonreuters.com/answerson/business-transparency-financial-crime/

[6] Juliette Garside, "Hundreds of Properties Could Be Seized in UK Corruption Crackdown," *The Guardian*, October 13, 2016, https://www.theguardian.com/business/2016/oct/13/properties-seized-assets-corrupt-cash-crackdown-criminal-finances-bill-tax-haven

allows the government to freeze the U.K. assets, including property, of international human rights violators, even if the offense was committed overseas.

The U.S. property market is similarly flawed. Earlier this year, as part of its program to identify and track secret homebuyers hidden behind shell companies and opaque structures for money laundering, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) found that "about 30 [percent] of the transactions covered by the Geographic Targeting Orders (GTOs) involve a beneficial owner or purchaser representative that is also the subject of a previous suspicious activity report. This corroborates FinCEN's concerns about the use of shell companies to buy luxury real estate in 'all-cash' transactions."[7]

Political commitments

Social pressure has finally pushed politicians to tackle the problem of secrecy. Unable to mask or ignore the impact that the lack of transparency in legal arrangements have on society, participants at the 2013 G8 Summit endorsed the core principles on beneficial ownership and published action plans setting out steps they will take to enhance transparency. In November 2014, G20 leaders adopted a policy document containing 10 principles intended to improve the transparency of beneficial ownership of companies and trusts—"G20 High-Level Principles on Beneficial Ownership Transparency." In the document, the group stated: "We need better cooperation between government agencies, as well as greater transparency, particularly on the beneficial ownership of corporations, trusts, foundations and other legal arrangements. We need to ensure that beneficial owners are identified and that access to information on beneficial owners and international exchange of this information can be further improved."[8] In June 2017, in Hamburg, the group again expressed the will for effective implementation of the international standards of transparency and UBO, welcoming the work done by FATF and the Global Forum on Transparency and Exchange of Information for Tax Purposes in this regard. The Group praised the "major progress" in the fight against tax evasion and tax avoidance, as reported by the Organisation for Economic Cooperation and Development in the July 2017 Report.[9] The development in the Base Erosion and Profit Shifting (BEPS) package implementation and first automatic exchanges of financial account information (AEOI), scheduled to take place in September 2017, were presented as the Group's recent achievements. However, in terms of the accessibility of the beneficial ownership information itself, not much has been presented in the G20 Hamburg Action Plan or the Leaders' Declaration, but further reports on the progress were requested.

As important as high-level political commitments are, progress in implementing changes at the national level has been unimpressive. Regulatory and legislative pressure to identify the UBO as part of AML and ABC regimes is growing. For example, regulators have taken more industries into their purview. However, governments have not made much real effort to make the information available.

Available information in the EU and the U.S.

In the EU, the Fourth AML Directive requires member states to introduce registrars of the beneficial owners of companies. Yet in June 2017 (the implementation deadline) only a handful of member states had functioning registrars. Most registrars were hidden by a paywall or simply unavailable to the public, with data protection and privacy laws cited to justify restricted access. For example, the U.K. beneficial ownership registrar ("People with Significant Control Registrar") opened in 2016, but excluded trusts from the requirement to file ownership information. Only a year later, Scottish Limited Partnerships (SLPs), which form two-thirds of all the opaque corporate entities in the U.K., have been covered by stricter disclosure rules. The registrar of trusts' beneficiaries is still to be created.

Where registrars did become available in Europe, the quality of data (often collected but not verified) was widely criticized by industry experts. This further illustrates that European countries still have a long way to go to make a real change. The beneficial ownership data that is collected must be of better quality, accessible without restrictions and encompassing of more legal forms, including trusts. Only then will European legal entities become unattractive to financial criminals.

The U.S. is only now attending to the problem. The International Monetary Fund strongly criticized the U.S. for failing to address the lack of transparency of American corporations and trusts, and published clear and strong recommendation for U.S. authorities to "ensure that accurate beneficial ownership information of U.S. corporations and trusts…is collected and maintained by either registries of corporations and trusts…and requiring all FIs and DNFBPs, in particular trust and company service providers (TCSPs) including lawyers and accountants providing such services, to identify the beneficial owners of

[7] "FinCEN Renews Real Estate 'Geographic Targeting Orders' to Identify High-End Cash Buyers in Six Major Metropolitan Areas," FinCEN, February 23, 2017, https://www.fincen.gov/news/news-releases/fincen-renews-real-estate-geographic-targeting-orders-identify-high-end-cash

[8] "G20 High-Level Principles on Beneficial Ownership Transparency," G20, 2014, http://www.g20.utoronto.ca/2014/g20_high-level_principles_beneficial_ownership_transparency.pdf

[9] "OECD Secretary-General Report to G20 Leaders," G20, July 2017, http://www.oecd.org/tax/oecd-secretary-general-tax-report-g20-leaders-july-2017.pdf

corporations and trusts and take reasonable measures to verify those identities."[10] A similar conclusion was made by FATF's U.S. AML/CTF framework assessment in 2016. Even though the overall evaluation was positive, there were two significant gaps found in the regime: exclusion or limited obligations for non-FIs and service providers, and a lack of timely access to current and accurate beneficial ownership information for regulators and law enforcement.

This criticism seems to be having an effect. In June 2016, FinCEN finalized its long-outstanding beneficial ownership rule, which extends customer due diligence requirements under Bank Secrecy Act (BSA) rules to the natural persons behind a legal entity. In addition, a new bill, the "Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017," has been recently proposed. This would introduce a new offense regarding the concealment of the source of funds in a transaction, including when such a source is a foreign politically exposed person, family member, or a close associate. The proposal stipulates penalties of up to 10 years' imprisonment, up to a $1 million fine, or both.

In June 2017, a bipartisan group of U.S. lawmakers introduced the Corporate Transparency Act, which would require FinCEN to collect information on the beneficial owner(s) of companies incorporated in the U.S. if the information has not been collected at the state level. Another group of lawmakers has also introduced the True Incorporation Transparency for Law Enforcement Act, a similar piece of legislation, which would instead have states collect the information.

Summary

While governments are debating the form and scope of collecting beneficial ownership information, FIs and DNFBPs, covered by know your customer rules under AML and ABC regimes, are already obligated to collect and verify that information. However, while information disclosed by the customer is insufficient, other sources of information are rare in most locations. Among jurisdictions that allow online or in-person retrieval of corporate registry information, only 36 percent provide direct shareholding information. Even after the Panama Paper revelation, little has changed. Only a handful of countries have improved accessibility to information. Regulators expect FIs to stand against financial crime, but they do not facilitate the fight by making the corporate date, including the ownership information, accessible to all. If governments do not follow through with their commitments to eradicate anonymous corporate vehicles and if obscure international structures are not honored, criminals will continue to hide behind them. Our role as members of civil society remains critical in demanding that follow-through.

Sylwia Wolos, CAMS, head of EDD proposition, Thomson Reuters, London, U.K., sylwia.wolos@thomsonreuters.com

[10] "Financial Sector Assessment Program," International Monetary Fund, June 2015, http://www.imf.org/external/pubs/ft/ scr/2015/ cr15170.pdf

Why the anti-financial crime community is strongly positioned for a centralized cross-institutional **artificial intelligence** platform

In the present environment, roughly one in three organizations experience economic crime, only 50 percent of money laundering or terrorist financing occurrences are identified by system alerts and one in five banks are recipients of regulatory enforcement actions.[1] The United Nations Office on Drugs and Crime found that "the estimated amount of money laundered globally in one year is 2 to 5 [percent] of global GDP, or $800 billion to $2 trillion in current U.S. dollars."[2] Likewise, before the end of 2017, compliance spending on anti-money laundering initiatives is expected to exceed $8 billion, a compounded annual growth rate of almost 9 percent.[3]

[1] "Adjusting the Lens on Economic Crime: Preparation Brings Opportunity Back into Focus," PWC, 2016, http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

[2] "Money Laundering and Globalization," UNODC, https://www.unodc.org/unodc/en/money-laundering/globalization.html

[3] "Adjusting the Lens on Economic Crime: Preparation Brings Opportunity Back into Focus," PWC, 2016, http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Given the magnitude of financial crime and the consequences of not getting ahead of it, regulated financial institutions (FIs) and others within the anti-financial crime community (such as government agencies and affiliates committed to financial crime detection and prevention) need to consider more disruptive and collaborative anti-money laundering and sanctions-related (collectively AML[4]) strategies. This includes actively exploring and understanding the possibilities associated with openly sharing resources and moving beyond a siloed approach to fuel more advanced, bolder technology-based AML tactics.

One route is to pursue the creation of a centrally-managed artificial intelligence (AI) tool that can be shared across and developed by multiple institutions in a controlled manner with an independent organization (such as a self-regulatory organization or a government agency) facilitating, governing and overseeing the process. This may be achieved by leveraging and combining three existing strategies: collaboration, centralization and investment in advanced technology.

A closer look at these three strategies and the potential applications of AI as it relates to AML, demonstrates why the anti-financial crime community may be ready for the next level in developing and using technology-based solutions in a collective, open source fashion.

Leveraging three existing risk management strategies

To get the upper hand in the fight against crime while demonstrating strong business practices and smart investment decisions, FIs need to be better and faster at employing technology to assist with job functions. Fortunately, there are three current techniques (collaboration, centralization and investment in advanced technology) that if used together in a new way may facilitate the development and use of AML-related technology within FIs. The following is a brief depiction of each of these areas as they relate to AML.

Collaboration

As demonstrated in legislation, government advisories and industry forums, AML advocates recognize that they have an important tool at their disposal: the "power of many."

Sections 314(a) and (b) of the USA PATRIOT Act are commonly referenced when demonstrating the importance of collaboration among the anti-financial crime community. Section 314(a) codifies the provisions relating to information sharing between law enforcement and FIs. The Office of the Program Manager for the Information Sharing Environment, noted that "Law enforcement information sharing has expanded significantly…improving law enforcement's ability to detect, prevent, and respond to acts of terrorism.... A fundamental component of effective enterprise-wide information sharing, for example, is the use of information systems that regularly capture relevant data and make it broadly available to authorized users in a timely and secure manner.… Criminal history records, law enforcement incident reports, records of judicial actions and decisions, and watchlists of known and suspected terrorists are all essential sources of vital data that provide accurate, timely, and complete information…"[5] Section 314(b), as FinCEN describes, "provides [FIs] with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities…. FinCEN strongly encourages information sharing.…"[6]

OUR NATIONAL SECURITY DEPENDS ON OUR ABILITY TO SHARE THE RIGHT INFORMATION, WITH THE RIGHT PEOPLE, AT THE RIGHT TIME

Former President Barack Obama had this to say in a National Strategy for Information Sharing and Safeguarding letter published in December 2012: "Our national security depends on our ability to share the right information, with the right people, at the right time. This information sharing mandate requires sustained and responsible collaboration between federal, state, local, tribal, territorial, private sector, and foreign partners."[7]

More recently, FinCEN reiterated the importance of collaboration in the context of cybersecurity in an October 25, 2016 advisory: "[FIs] can work together to identify

[4] Refers to Bank Secrecy Act (BSA), anti-money laundering (AML) and Office of Foreign Assets Control (OFAC) activities.

[5] "Law Enforcement Information Sharing," Information Sharing Environment, https://www.ise.gov/law-enforcement-information-sharing

[6] "Section 314(b) Fact Sheet," FinCEN, https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

[7] "National Strategy for Information Sharing and Safeguarding," Council on Foreign Relations, December 1, 2012, http://www.cfr.org/intelligence/national-strategy-information-sharing-safeguarding-2012/p31630

BY HAVING STANDARDIZED PROTOCOLS, PRACTICES AND REPOSITORIES OF INFORMATION, FIs ARE ABLE TO MAINTAIN CONSISTENCY, COHESIVENESS AND TRANSPARENCY IN THEIR OPERATIONS

threats, vulnerabilities, and criminals. By sharing information with one another, [FIs] may gain a more comprehensive and accurate picture of possible threats, allowing for more precise decision making in risk mitigation strategies." Specifically, FinCEN notes that "collaboration and ongoing communication among BSA/AML, cybersecurity, and other units will help [FIs] conduct a more comprehensive threat assessment and develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime."[8] FinCEN further notes that FIs "are encouraged to internally share relevant information from across the organization…information provided by cybersecurity units could reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units… such as patterns and timing of cyber-events and transaction instructions coded into malware…to 1) help identify suspicious activity and criminal actors and 2) develop a more comprehensive understanding of their BSA/AML risk exposure."[9]

While there is already a strong inclination among FIs to share select information with each other and government agencies, the extent of this sharing and collaboration could not only be expanded, but also made more reciprocal in nature. For instance, FIs can share entire data sets with each other and government agencies can also share certain data of their own with FIs.

Centralization

Centralization, for the purposes herein, refers to the act of consolidating and managing AML processes, procedures, functions or systems centrally, such as by designating a primary unit, utility, or hub to manage a specific activity.

In the context of managing risk by centralizing functions and processes, the Federal Financial Institutions Examination Council explains the following: "risk assessment, internal controls (e.g., suspicious activity monitoring), independent testing, or training may be managed centrally. Such centralization can effectively maximize efficiencies and enhance assessment of risks and implementation of controls across business lines, legal entities and jurisdictions of operation. For instance, a centralized BSA/AML risk assessment function may enable a banking organization to determine its overall risk exposure to a customer doing business with the organization in multiple business lines or jurisdictions."[10]

Similarly, the benefits of a standardized approach apply to guidance and procedures. By having standardized protocols, practices and repositories of information, FIs are able to maintain consistency, cohesiveness and transparency in their operations.

Creating a "holistic" (or enterprise-wide) view, which is often an intended result of centralization, is also encouraged within the industry. For instance, regulators have explained that in order to obtain a more accurate understanding of a client base,

[8] "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," FinCEN, October 25, 2016, https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

[9] Ibid.

[10] "BSA/AML Compliance Program Structures—Overview," FFIEC, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_039.htm

customer relationships should be reviewed holistically across lines of business, with a comprehensive approach to quantifying BSA/AML risk for new and existing customers, and that "the quantification of risk [should] encompass a customer's entire relationship."[11]

Consequently, a centralized, yet interconnected approach that provides a holistic view and governance model (e.g., one that consolidates a function into a central utility while maintaining communication and awareness with respective business lines), allows for better identification and management of risk, enhanced communication, and a setting more conducive to internal and external testing and evaluation.

Investment in Advanced Technology

With the growth of technology rapidly increasing, FIs have been employing techniques such as advanced analytics and automation to assist with performing key AML functions (e.g., know your customer activities, transaction monitoring, list screening). While these strategies continue to evolve and work well with structured data sets (e.g., information organized into specific fields or formats) and prescriptive functions (e.g., defined rules and scenarios), FIs are also looking at bolder technology solutions, such as AI (referred to herein interchangeably with the terms "cognitive technology" and "cognitive computing"), to tackle more complex and analytical areas, including unstructured data sets (e.g., unorganized or non-text information).

Cognitive computing refers to the simulation of human thought processes, using self-learning systems that include data mining, pattern recognition and natural language processing to mimic the way the human brain works.[12] This allows a computer to derive conclusions and complete activities that may require fundamental human skills and intelligence, such as looking, reading, writing and integrating knowledge. Machine learning, which works by using algorithms that iteratively learn and adapt in an automated manner as the models are exposed to new data, is a method used to enable a computer to learn without being programmed.[13]

One attractive advantage of cognitive technology is the ability to access, make sense of, and/or use large, unstructured and diverse information, including non-traditional information such as social media information (e.g., posts, images) and audio (e.g., telephone conversations) that may be available in other parts of an FI (e.g., the marketing department or customer service) for AML purposes. A more ambitious goal is the potential to be predictive, rather than reactive, in identifying fraudulent activity, such as by recognizing traces of the behavior before it fully occurs through enabling computers to learn, comprehend and detect new money laundering schemes and characteristics.

A glimpse at how cognitive technology is being applied within AML

On February 15, 2011, an IBM-developed supercomputer with AI, named Watson, capable of answering questions in natural language, won the first place prize of $1 million on the quiz show, *Jeopardy*.[14]

Five years later, on March 8, 2016, KPMG LLP, a "Big Four" audit, tax and advisory firm, revealed plans to leverage IBM's cognitive computing technology explaining that "[a]uditing and similar knowledge services are increasingly challenged with tackling immense volumes of unstructured data. Cognitive technologies such as Watson can transform how this data is understood and how critical decisions are made." For example, "cognitive technology is further advancing improvements to sampling processes, in which auditors review subsets of data to analyze thousands or millions of actions to draw conclusions."[15]

On November 22, 2016, it was announced that Promontory Financial Group, a risk management and regulatory compliance consulting firm with a global AML and counter-terrorist financing practice, was acquired by IBM. Promontory's professionals intend to train Watson via machine learning. For instance, Watson will learn by "continuously ingesting regulatory information as it is created and through interaction in real-world applications. This includes solutions for tracking evolving regulatory obligations, expectations and control requirements, as well as solutions that address specific compliance needs, such as financial risk modeling, surveillance and insider threat, and financial crimes including counter fraud, [AML] and [KYC]."[16]

In addition, a 2016 research report from Celent (a research and advisory firm focused on business and technology strategies) examined AI applications, vendor profiles, and application trends, and noted that AI "technologies are increasingly being applied in the banking industry, mainly toward knowledge management, identity authentication,…anti-money laundering, and risk control." In reference to AI, the report further notes that "[w]ith their ability to fully understand the market, customers, and regulatory changes through data, banks are in the best position to apply these technologies..."[17]

[11] "Consent Order," U.S. Department of Treasury Comptroller of the Currency," 2015, www.occ.gov/static/enforcement-actions/ea2015-113.pdf

[12] "Cognitive Computing," http://whatis.techtarget.com/definition/cognitive-computing

[13] "Machine Learning," SAS, http://www.sas.com/en_us/insights/analytics/machine-learning.html

[14] John Markoff, "Computer Wins on 'Jeopardy!': Trivial, It's Not," *New York Times,* February 16, 2011, http://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html?pagewanted=all&_r=0

[15] "KPMG Announces Agreement with IBM Watson to Help Deliver Cognitive-Powered Insights," IBM, https://www-03.ibm.com/press/us/en/pressrelease/49274.wss

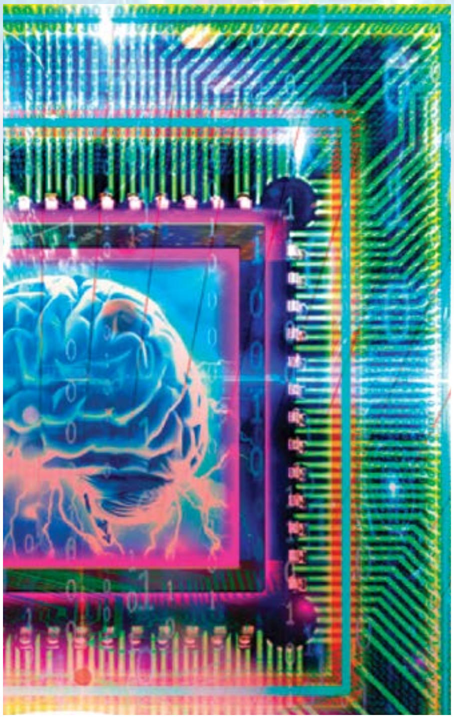
[16] "IBM Closes Acquisition of Promontory Financial Group," Promontory, November 22, 2016, http://www.promontory.com/News.aspx?id=4392

[17] Hua Zhang, "Artificial Intelligence in the Banking Industry: From Data Analysis to Semantic Analysis," Celent, July 13, 2016, http://celent.com/reports/artificial-intelligence-banking-industry-data-analysis-semantic-analysis

Accordingly, new AML software, products and tools with AI technology are quickly entering the market to assist FIs with complex AML activities, such as identifying and evaluating suspicious activity. For instance, existing AI technology has the ability to track the behavior of individuals and entities involved in potential money laundering activity and link them to one another through collective intelligence gathering and machine learning techniques that apply adaptive learning rather than predefined scenarios and rules.[18] This method can provide a stronger and more comprehensive understanding of behavior over time. Other machine learning-based platforms have the ability to identify and aggregate voluminous and unstructured data points, such as narratives within SARs or publicly available information, to assist with better recognizing AML risks and automating KYC processes.[19]

Taking a leap: Go bold to get ahead

The evolving partnerships with technology companies, such as IBM and the many vendor products entering the market, illustrate the applications and benefits of cognitive technology in the AML space, particularly as technology becomes cheaper and the demand for skilled labor increases. The value of cutting-edge technology and "digital labor" combined with the growing importance of collaboration and centralization presents opportunities for how FIs can begin to implement, experiment with, or simply think about how to leverage cognitive computing capabilities through a transformative framework or methodology that encourages communities that are against financial crime to operate as partners in a common cause.



For instance, a centralized cognitive computing tool that incorporates multiple FIs (in a structured, yet cooperative fashion similar to crowdsourcing, where participants collectively contribute to, and benefit from, pooled information and knowledge) fits well with the ongoing emphasis on collaboration, centralization, and investing in technology. A basic benefit would be a more powerful data set (e.g., aggregated KYC and transactional activity) with an integrated feedback loop that links back to the originating FIs, allowing for enhanced data quality and analysis. The tool could serve as a supplemental data store that FIs can use side by side with existing mechanisms to validate or complement current data; and/or provide future potential to feed directly into the FIs' systems and/or models.

While similar tools exist in the form of vendor products and AML collaboration software, an option of taking this even further is a semi-communal cognitive computing tool that is managed centrally by an independent third party (such as a self-regulatory organization or a government agency). By identifying an appropriate third-party candidate with sufficient technological capabilities and dedicated resources, the organization would be able to provide oversight, as well as set up and pilot the tool in a safer and more focused environment. This form of centralization may also be more cost-effective, time-efficient and supportive for FIs, as it allows the effort to be shared and distributed. For instance, this unit could maintain governance over the tool and assist with coordinating the retrieval of information from participants, as well as cleansing and anonymizing data where necessary.

Although the initial investment (such as the time and funding associated with development and integration) for a centralized cross-institutional AI platform may seem daunting, the long-term benefits are likely to outweigh these immediate costs, particularly if pursued earlier, given the current state of the AML landscape and the nature of technological growth. More importantly, this path could potentially foster more rapid and effective technological advancements of similar tools within the AML space and pave the way for a new type of expanded partnership and alliance among opponents of financial crime: one that helps FIs get ahead and stay ahead. A

Jonathan Estreich, CAMS-Audit, CFE, director, Société Générale, New York, NY, USA, editor@acams.org

The author submitted this piece while an employee of JPMorgan Chase. The views expressed in this article are those of the author and do not represent the views or opinions of JPMorgan Chase or Société Générale.

[18] "Next Generation, Artificial Intelligence and Machine Learning," Brighterion, http://brighterion.com/next-generation-artificial-intelligence-machine-learning/

[19] "Unstructured Data: Delivering Precision and Productivity to the AML Team," Digital Reasoning, http://www.digitalreasoning.com/resources/AML-KYC.pdf

議反洗錢管理之“風險為本”

澳門反洗錢師專業協會張帆副理事長

一、“風險為本”簡析

“風險為本”（Risk-based）反洗錢原則最早由英國監管機構宣導，英國金融監管局（FSA）最早在2000年1月制定的《新千年的新監管者》提出這一理念。隨後，被沃爾夫斯堡集團（ Wolfsberg Group）、金融行動特別工作組（FATF）、國際保險監督官協會（IAIS）、國際證券委員會組織（IOSCO）等國際組織積極宣導。2012年2月，FATF新的《反洗錢、反恐怖融資和反擴散融資國際標準》（新40項建議）明確了以風險為本的反洗錢工作原則，最終成為國際反洗錢領域的變革方向。“風險為本”原則簡而言之，就是要求金融機構對本機構面臨的洗錢、恐怖融資等非法活動的風險高低進行評估，進而合理配置相應的資源，有輕重、有主次地採取相應的控制措施。

The “risk-based” principle of AML management

The “risk-based” anti-money laundering (AML) principle was first promoted by British regulatory authorities. In January 2000, the Financial Services Authority (FSA) was the first to put forth such a concept in its book titled *A New Regulator for the New Millennium*. Since then, the principle was actively promoted by international organizations, such as the Wolfsberg Group, the Financial Action Task Force (FATF), the International Association of Insurance Supervisors and the International Organization of Securities Commissions. In February 2012, FATF published its updated “International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation” (the revised FATF 40 Recommendations) which clearly defines the risk-based AML principle, ultimately ushering in an era of revolutionary change in the international AML arena. Simply put, the “risk-based” principle requires financial institutions to assess the risks associated with illicit activities (such as money laundering and terrorist financing) that they may face in order to reasonably deploy corresponding resources before taking prioritized control measures as a response to these risks.

二、“風險為本”的必要性

客觀的說，由於不同國家/地區的經濟結構各有特點，反洗錢監管規則、反洗錢管控意識和管控水準、階段性打擊力度等也往往存在差異，洗錢者總是努力給黑錢找“出路”，這些黑錢就可能會從管理較嚴的機構/地區向管控較弱的機構/地區轉移，從管理完善的業務領域向管理尚不成熟的業務轉移，即“短板效應”。例如，早前一段時間歐洲部份國家先行加強了現金存款業務的審查與管理，洗錢者們便駕車把鉅額現金運至管控較松的國家。再如，第三方支付蓬勃發展，加速了資金匯劃，使資金鏈條複雜化，而反洗錢監管未及時到位，客戶及交易信息傳遞不足，銀行就需要更多地關注此類交易的洗錢風險。

可見，與“規則為本”被動地執行監管規則與標準相比，“風險為本”是需要銀行主動識別、發現黑錢的各種“出路”與變化，進而找出方法去防控。

三、“風險為本”之關鍵

銀行業要落實“風險為本”原則，必須將反洗錢管理的重心由事後分析判斷向事中主動管理轉移，就需要將風控理念、機制、要求與銀行業務拓展經營有機結合；建立起嚴格的反洗錢合規原則，運行全流程、統一的風險管理機制，進而在集團範圍樹立良好的合規管理文化。

（一）客戶盡職調查是管理基礎

起初，銀行尤其是全功能銀行對普通客戶的資訊收集相對簡單，對有業務服務（比如授信、理財等）的客戶資訊收集相對豐富，但此類客戶占比並不高，所以應當承認銀行並不瞭解大部份客戶。因此，許多銀行因反洗錢違規被監管施以鉅額處罰後，評估比較了盡職調查成本和經營收益，主動選擇退出低值客戶、低盈利區域，把精力集中於維護高值客戶。同時，銀行業務人員即使在業務過程中收集到客戶、業務信息，但受到個人風險管理意識和技能所限，無法充分運用於管理。加之系統功能不支持等，均限制了銀行清晰記錄展示、準確分析評估客戶洗錢風險。

The necessity of the “risk-based” principle

Objectively speaking, as different countries/regions have unique economic structures, more often than not there are variations in AML regulatory requirements, AML control awareness and capabilities, as well as the amount of AML efforts. Money launderers are always painstakingly scrambling to find new “outlets” for black money, and such black money may be transferred from institutions/regions with more stringent management to those with weaker management or from business areas with sound management to those with immature management (“buckets effect”). For example, after some European countries a while ago took the initiative in tightening their audit and management on cash deposit operations, money launderers drove their truckloads of money to other countries with relatively lax controls. Furthermore, the booming development of third-party payment expedites capital transfer and remittance, complicating the flow of funds. On the other hand, banks need to pay more attention to money laundering risks associated with these kinds of transactions owing to AML regulatory controls that fail to keep up and insufficient communication in customer and transaction information.

It is evident that the “risk-based” AML approach requires banks to proactively identify and seek out various “outlets” and changes of black money in order to find ways to control money laundering, whereas the “regulation-based” approach only requires passive enforcement of regulatory requirements and standards.

The key to the “risk-based” principle

To implement the “risk-based” principle, the banking industry needs to shift the focus of AML management from post-analysis and judgment to proactive management. With this in mind, banks must organically integrate risk control ideas, mechanisms, requirements and banks’ business development and management. Banks need to build up stringent AML compliance principles and enforce whole processes and unified risk management mechanisms, in order to establish a sound and compliant management culture within the institutions.

Customer due diligence is the basis of AML management

Previously, banks—particularly full-service banks—took things lightly when it came to collecting information about their ordinary customers. They tended to collect information about customers of business services (such as credit granting and money management, etc.) but these customers only accounted for a small fraction of their clients. So, it is fair to conclude that banks did not know the majority of their customers. Therefore, many banks were penalized by regulators for the violation of AML regulations. In response, they proactively decided to divert their focus from low-value clients and regions with low profitability to high-value clients, after weighing customer due diligence (CDD) costs against operating income. In the meantime, even if banking staff managed to collect information on customers and their transactions, they were still unable to apply them to AML management due to the lack of risk management awareness and expertise. In addition, the unavailability of support

而準確判斷客戶洗錢風險等級是“風險為本”首要條件。銀行需要從業務、行業、客戶特徵、地域等維度開展盡職調查，得到充分、完整、真實的客戶資訊，作為分析基礎。除了客戶自身的信息，銀行還需要瞭解更多的資訊，比如業務經營範圍、主要交易對手、交易地區、交易幣種、交易規模、實際受益人、負面新聞等。這些工作應當嵌入到客戶關係准入、維護等流程，成為業務日常管理內容之一。各業務單位要樹立全面風險管理意識，不應把反洗錢要求的對客戶、交易的調查，與日常業務（比如授信、貿易融資等）過程中的客戶盡職調查相互獨立，而應將洗錢風險作為審視評估客戶和業務的維度之一，與信用風險、市場風險、操作風險等業務管理措施逐步融合。然後，後線風險管理人員才能基於這些資訊，運用專業工具去評估風險，制定出更有針對性的管控措施。

（二）即時交易監控是重要方法

客戶的洗錢風險評級結果應當得到妥善應用，其中之一就是即時交易監控或限制。對於特定類型客戶或高風險客戶，銀行應當結合其風險特徵，在業務系統中增加交易監控或限制安排，例如對於頻繁存入現金的客戶增加需要強化盡職調查的提示，對於經分析存在異常跨境交易的客戶增加匯入或匯出匯款總額的限制，對於存在網路欺詐嫌疑的客戶限制其使用電子、第三方支付等自助渠道，等等。反洗錢早已不再簡單的是事後可疑交易報告，它要求銀行主動管理風險，控制潛在風險的發生。

> AML IS NO LONGER JUST ABOUT REPORTING SUSPICIOUS TRANSACTIONS AFTER THEIR OCCURRENCES; IT REQUIRES BANKS TO PROACTIVELY MANAGE RISKS AND CONTROL THE OCCURRENCE OF POTENTIAL RISKS

by system functions further restricted banks' capability to clearly document, demonstrate and accurately analyze risks associated with customer money laundering.

Accurately judging the risk level of customer money laundering is an important prerequisite for the "risk-based" approach. Banks need to conduct due diligence on business operations, industries, customer characteristics and regions, in order to obtain adequate, complete and truthful customer information as the basis of analyses. In addition to information pertaining to customers themselves, banks also need to obtain more information, such as the scope of business operations, their major counterparties, transaction areas, transaction currencies, transaction scale, actual beneficiaries and negative news. These efforts should be embedded into the procedure for the establishment and maintenance of customer relationship, thus becoming part of daily business operation management routines. When trying to build up sweeping risk management awareness, business operation units are advised against separating the investigation on customers and transactions as required by AML from CDD during the course of routine business operations (such as credit granting and trade financing, etc.). Instead, they should consider the risk for money laundering as one of the angles for examining customers and business operations, while driving the gradual integration of various business operation management measures such as credit risks, market risks and operational risks. With these efforts in place, backline risk managers can utilize professional tools to assess the risks for money laundering and formulate specific control measures based on this information.

Monitoring real-time transactions is a key method

A customer money laundering risk rating should be properly applied. One of the applications is the monitoring of or restrictions on real-time transactions. With regard to specific types of customers or high-risk customers, banks should combine their risk characterization to increase monitoring or restriction measures in their business operation systems. For example, adding a prompt for enhanced due diligence on customers with frequent cash deposits; putting a limit on incoming and outgoing remittance for customers who have had unusual cross-border transactions according to analyses; restricting the use of self-help channels such as electronic and third-party payment by customers suspected of internet fraud, etc. AML is no longer just about reporting suspicious transactions after their occurrences; it requires banks to proactively manage risks and control the occurrence of potential risks.

Money laundering risk assessment on products is a necessary approach

Banks must assess the money laundering risks for various products, ensuring that the control measures for different products are appropriate and that existing risks are brought under control. Therefore, banks need to incorporate a money laundering risk assessment into their product management systems, in addition to building product risk heat maps, regular reexamination in conjunction with business conditions and the adjustment of assessment conclusions as needed. When competitors or other banks identify that a particular

（三）產品洗錢風險評估是必要手段

銀行必須評估各類產品的洗錢風險，明確不同產品的管控措施是否得當、固有風險有無得到控制。因此，銀行要將洗錢風險評估納入在產品管理體系中，建立產品風險熱圖，定期結合業務情況重審、調整評估結論。當同業或銀行發現某一產品容易被利用于洗錢，或者控制措施未達到預期目標，應當及時啟動觸發式評估，調整產品風險等級，優化管控措施，進而決定是否停辦該產品。目前，銀行在產品風險評估及管理實踐中遇到的主要問題：一是如何準確計算產品風險，現有銀行的產品分類、財務覈算等方法有些地方不適用於反洗錢評估，產品效益、客戶群等許多數據無法直接取得、分析；二是何時以何標準啟動觸發式評估。這些都涉及銀行管理機制的調整與優化。

（四）先進資訊技術不可或缺

隨著“風險為本”管理深入，反洗錢系統功能必須強大，這不僅是人工成本投入的考慮，更是提高分析監控準確性的要求，對於客戶群、日常交易規模大的銀行尤其重要。無論是可疑交易案例精准度的提高，制裁名單過濾誤中率的減少，還是客戶盡職調查、交易限制等對於業務流程的參與，早已是人工憑著經驗、記憶無法實現的，要提高風控能力需要更加離不開系統支持。僅僅“黑名單”篩查也已從制裁名單和政要人士，擴大至各類負面信息、船舶與港口、軍民物資清單等海量資訊處理。隨著近年來大數據不斷推廣應用，各種信息服務商、互聯網平臺相應而生，讓迅速處理海量資訊、抓取有價值的信息成為可能。資訊技術是銀行真正意義地建立并運行“風險為本”合規管理機制不可或缺的工具。

在國際經濟交流頻繁、資金全球即時互通的新時期，洗錢模式層出不窮，強化反洗錢管理已成為監管和銀行的共識。銀行想要強化反洗錢管控，就必須將“風險為本”原則扎扎實實地嵌入到經營管理之中，融匯到員工意識之中。

product is prone to be exploited for money laundering or control measures have failed to live up to their expectation, banks should initiate a triggering assessment to adjust product risk levels and to optimize control measures in order to decide whether or not to suspend a product. At present, major problems encountered by banks in terms of the realization of product risk assessment and management are the following:

1. How can banks accurately calculate product risks? Some of banks' existing methods for product categorization and financial accounting are partly unsuitable for AML assessment. For example, many figures such as product effectiveness and customer bases cannot be directly accessed and analyzed.
2. When and based on what criteria should banks decide to initiate the triggering assessment?

These problems involve the adjustment and optimization of banks' management mechanisms.

Advanced information technology is a must

As we strengthen "risk-based" AML management, the AML system's functions must be robust, which involves not only the consideration for labor cost investment, but also an improvement in accuracy for analysis and control. It is especially important for banks with a large scale of customer bases and daily transactions. No matter if it is about increasing the accuracy of suspicious transaction reports, reducing the rate of missed hits in screening a sanctions list, or a business procedure participation in CDD and transaction restrictions, people armed with only experiences and memories can no longer get the job done. In order to increase risk control capabilities, system support is more and more indispensable. Even the screening for a "black list" has expanded from a sanctions list and political dignitaries to big data information processing of various negative news, ships, boats and harbors, as well as military and civilian material checklists. As the application of big data continues to expand in recent years, various information service providers and internet platforms have emerged as a result, making it possible to process big data and capture valuable information. Information technology is an indispensable tool for banks to truly build and enforce a "risk-based" compliant management mechanism.

In the new era of frequent international economic exchanges and instantaneous global capital interflow, new money laundering models continue to mushroom. It has become a consensus among regulators and banks to enhance AML management. If a bank wishes to enhance its AML control, it needs to solidly embed the "risk-based" principle into its operations and management, while ingraining it into the awareness of its employees.

Zhang Fan, CAMS, vice chairman, Macau Anti-Money Laundering Specialists Association, Bank of China, Macau, zhang_fan@bocmacau.com

EU challenges: What is new?

Editor's note: European Connect is a section in the ACAMS Today magazine that will update members on ACAMS news and activities in Europe.

Lately, the EU has been ramping up its focus on preventing financial crime, with regulators creating entirely new paradigms for organizations operating here and the press reporting the industry's news on its front pages, not the financial ones.

Particularly challenging for organizations in Europe is aligning their operations across the multiple jurisdictions in which they are based. At the time of this writing, there are indications that the U.K. will enforce a different sanctions regime to the EU post-Brexit that will increase the complexity of managing sanctions risk—an already complicated area.

This year, the European Parliament has also rejected a blacklist of countries prepared by the European Commission several times for relying too heavily on the Financial Action Task Force's own blacklist. Parliamentarians have recommended the Commission take more of a 'zero-sum' approach to drawing this up, as they believe it should be expanded (nationals from these countries will then be subject to greater checks when trying to do business in Europe).

However, an overarching trend we are seeing is transparency. Regulators are demanding it and organizations are struggling to balance that requirement alongside strict data protection regimes. The Data Protection panel at our 2017 European Conference was well attended and highly rated as attendees heard how big European organizations are managing that push and pull.

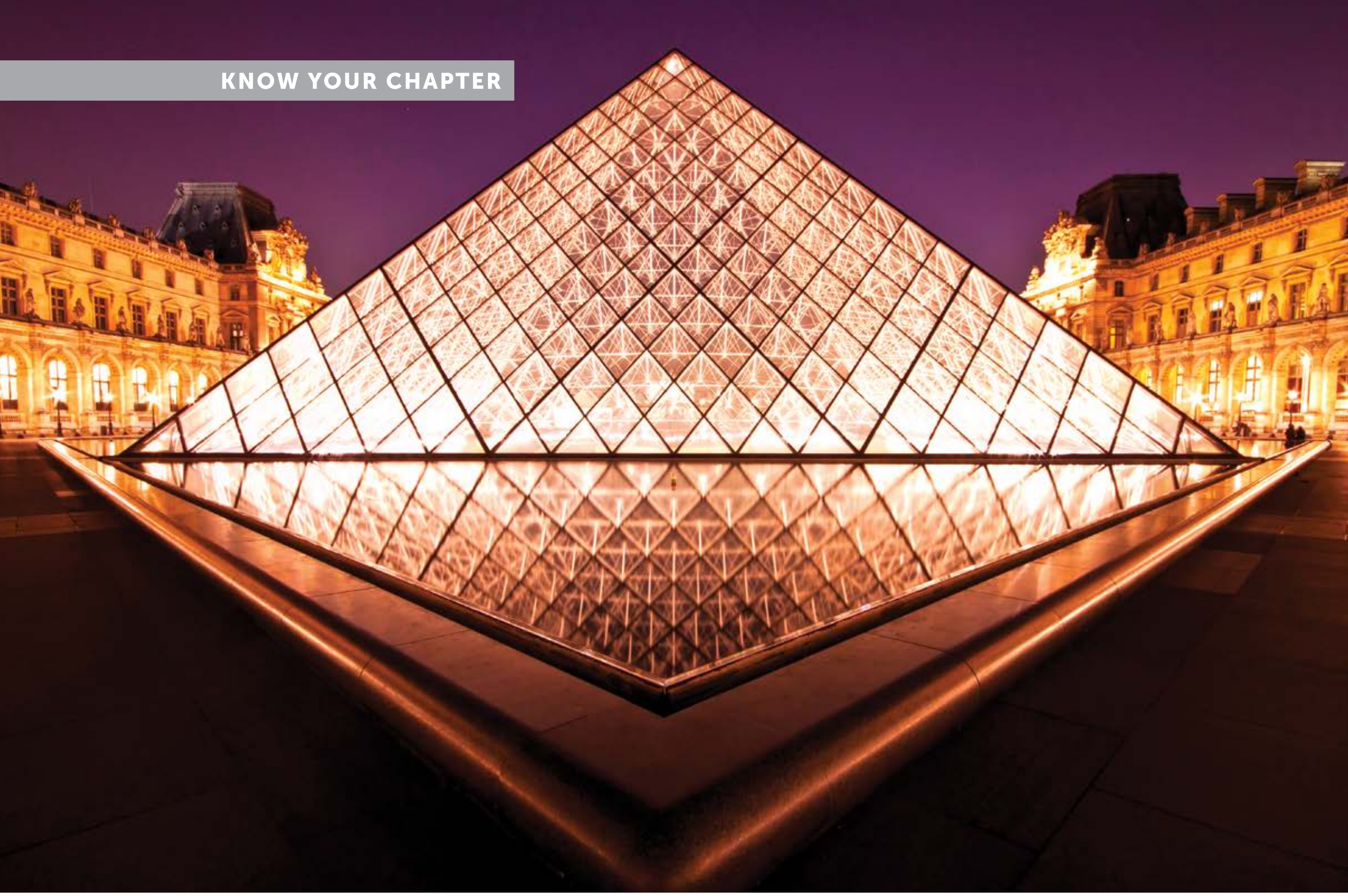
Finally, I wanted to give you the dates of our upcoming events in Europe:

- **Anti-Financial Crime Symposium–Ireland**
  Dublin, October 19, 2017
- **Anti-Financial Crime Symposium–Nordics**
  Copenhagen, November 16, 2017
- **KYC/CDD Boot Camp**
  London, December 7, 2017

Our European Chapters also continue to organize exciting networking and learning events, so I hope to have the chance to meet all of you somewhere in Europe soon.

Angela Salter, head of Europe, ACAMS, London, U.K., asalter@acams.org

Visit CSI
at booth 216-218
ACAMS
VEGAS!



Editorial credit: Tungtopgun/Shutterstock.com

SAPIN II—
A FIRST STEP TOWARD A EUROPEAN LAW ON CORRUPTION?

In December 2016, France adopted the Sapin II law. One might think of it as just another piece of law in the legislative jungle; however, it is not. Indeed, it is the first strong French anticorruption law and even though it might look, at first sight, as a pale copy of the U.S.' Foreign Corrupt Practices Act (FCPA),[1] the subject is worth a closer look.

▲ May 23, 2017—Paris:
France Chapter Conference on anti-corruption

[1] Foreign Corrupt Pratices Act, American anticorruption law. "The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. (FCPA), was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business," retrieved on June 20th, 2017, https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

May 23, 2017—Paris:
France Chapter Conference on anti-corruption

The man behind the French Anticorruption Act

At one of its regular events in Paris, on May 23, 2017, the France Chapter welcomed the man considered by many as being responsible for the law. The man, who wished to remain anonymous, was invited to the conference to tell his story. The audience, mainly consisting of Parisian representatives of the compliance community, silently listened to his harrowing testimony.

This former top executive of a major French industrial company explained how the FBI at the New York John F. Kennedy International Airport arrested him in April 2014 while he was on a routine business trip.

Arrested and handcuffed within the frame of the FCPA, his first thought was that he would spend a couple of hours in custody and be set free after what he then thought was a misunderstanding.

Unfortunately, months went by and he slowly had to get used to the day-to-day life of an American prisoner.

Stuck in the middle of a political and economic imbroglio, he had to plead guilty and was finally allowed to go home after spending 14 months in a federal state prison in the U.S., for allegedly being involved with a corruption case that occurred years ago.

What is Sapin II?

The French anticorruption law is all about transparency, anticorruption and the modernization of business life.

To ensure regulatory harmonization and consistency, Sapin II is an attempt to bring an answer to the powerful American FCPA and its European counterpart, the U.K. Bribery Act.

Sapin II creates a new authority (aka the National Anti-Corruption Agency) and protects internal whistleblowers. It also requires companies to comply with a set of eight anti-corruption measures, which include: the implementation of a code of conduct and a central register for all alerts related to corruption; a risk map of corruption risks; a risk assessment which identifies clients, suppliers and intermediaries risks; a specific training for adequate employees; a sanctions framework and an internal audit with which to ensure that the above mentioned measures are duly complied.

Failure to comply with the law can lead to a penalty amounting to 1 million euros or even 30 percent of the annual turnover of the company—taking its turnover of the last three years into account.

Last but not least, the law includes the introduction of the concept "judicial convention of public interest," which is a remake of the U.S. "deferred prosecution agreement."

What Sapin II is not

Although Sapin II can be regarded as the twin sister to the American FCPA, it is not the FCPA. While both laws aim to fight corruption, the FCPA has been applied, since 1998, to "foreign firms and persons who cause, directly or through agents, an act in furtherance of such a corrupt payment to take place within the territory of the United States."[2] This means that the FCPA applies to foreign firms as well as any act linked to the U.S. The scope is huge.

Sapin II could be regarded as the twin sister of the U.K. Bribery Act too. Here again the British piece of law is more ambitious since it applies to any foreign subsidiary on its soil, and by extension, to the group the subsidiary belongs to.

The French Sapin II is restricted to firms registered in France. It exclusively applies to companies whose head offices are registered in France and more specifically to all private companies and public companies employing more than 500 staff members and whose turnover is higher than 100 million euros.

In other words, FCPA is aggressive, the U.K. Bribery Act is half-aggressive, and Sapin II is exclusively defensive.

Conclusion

Although no one can deny that this anticorruption law is a big step forward for France, one can wonder whether this first action is to be followed by ones that are more ambitious. Will a more ambitious second act enhance this first attempt?

We will leave it with the businessman behind the Sapin II law, who shared his unfortunate experience with the ACAMS France Chapter community and closed the conference by reminding the audience that 25 years ago the EU adopted an antitrust law. The U.S. would then rely on such a law and the EU decided to enact its own legal antitrust infrastructure. Will the newly enacted Sapin II in France turn out the same way and have a European destiny? A

Nathalie Bosse, CAMS, communications director, ACAMS France Chapter, Paris, France, nbosse@acams.org

Dan Benisty, co-chair, ACAMS France Chapter, Paris, France, dan_benisty@hotmail.com

[2] Retrieved on June 20, 2017, from https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

Community bankers and the new CDD Rule

The goal of the Community Banking Corner is to provide useful tips for Bank Secrecy Act/anti-money laundering (BSA/AML) professionals in community banks to help them in their day-to-day jobs. This section will focus on all aspects of BSA/AML from the effects of de-risking on smaller banks to efficiencies that can help BSA/AML professionals in community banks. We plan to cover many topics in the *ACAMS Today* magazine and on ACAMSToday.org.

So, if you are a community banker with topic ideas you would like to discuss, please feel free to send them to robert.soniat@bankatunion.com.

Community bankers and the new customer due diligence beneficial ownership rule

Over the past year, banks have been preparing for the new customer due diligence (CDD) beneficial ownership rule, which should be implemented by May 2018.

From a community banker's perspective, here are a few key points that stand out:

- Specific attention has been paid to the beneficial ownership section of the rule. Although this is understandable since it is new to many community banks, it is important not to lose focus on other aspects of the regulation. It is especially important not to lose focus on the third and fourth parts of the regulation. Even though these items are not new to banks, they are now required and a review of current processes to update what is currently done may be necessary to ensure your bank is in compliance.
- Vendor relationships are a critical component of this regulation. While many AML vendors are on track to assist AML teams in their compliance efforts, many of the pain points community banks are feeling pertain to the development and support from core vendors and platform account opening vendors. Bankers find that the vendors are either not ready or their systems do not easily fit into the bank's process to comply with the regulation. It is important now more than ever to communicate with your banking peers and to share information to determine if system vendors in the financial sector have sufficient information. In addition, it is important to determine if they understand the needs banks have in order to comply with the regulation, with as little impact as possible to the process flow when opening and monitoring accounts.
- Determining what constitutes a trigger event. There has been much discussion on what is a trigger event, which as per the regulation requires, "the obligation to update customer information as a result of monitoring would generally only be triggered when the financial institution becomes aware of information about the customer in the course of normal monitoring relevant to assessing the risk posed by a customer; it was not intended to impose a categorical requirement to update customer information on a continuous or ongoing basis using the Certification Form in Appendix A or by another means."

  In my perspective, it is better to keep it simple and not have 20 to 30 documented items that are trigger events. Have a simple list of items, which prompt the bank to determine if the event or customer activity prompts an update to their risk profile.
- One of the biggest pain points is that updates to the FFIEC BSA/AML Examination Manual, detailing examiner requirements, have not been published as of yet and may not be out until late 2017 or early 2018. This puts those of us attempting to implement this regulation in the middle of a guessing game. While bankers are working to implement the requirements, they also hope their interpretations are closely aligned with the expectations of examination requirements.

Finally, one of the most important pieces of advice I tell other bankers is to try and think of this as a positive. With the new regulation you have a great opportunity to strengthen your institution's know your customer/CDD program, which is the backbone of a strong BSA/AML program. So, think about how you can accomplish this and implement strong changes to help your program become stronger.

Robert J. Soniat, CAMS-FCI, vice president—BSA/AML officer, Union Bank and Trust, Glen Allen, VA, USA, robert.soniat@bankatunion.com

Tanya Montoya: It's All About Risk Assessment

ACAMS Today spoke with Tanya Montoya, senior product development manager at ACAMS, about ACAMS Risk Assessment and human trafficking.

As senior product development manager for ACAMS, Montoya is responsible for the management and strategic oversight of ACAMS Risk Assessment®, the association's first risk assessment software designed to offer financial institutions worldwide, a standardized means of measuring, understanding and explaining their money laundering risks.

During her five-year tenure with the organization, Montoya has taken the product from inception to a full launch and forged strategic relationships and partnerships with key industry members in both the public and private sectors, comprised of anti-money laundering (AML) thought leaders from global financial institutions and banking regulatory authorities. In this capacity, Montoya is also responsible for the full governance and audit of this critical software tool as it relates to global AML best practices, guidance, regulation and cybersecurity. Through these endeavors, Montoya is able to extend her expertise and knowledge in the space to ACAMS Risk Assessment users that seek guidance in the application and implementation of the tool against their institution's own risk assessment obligations.

In addition to her principal responsibilities, Montoya chairs the *ACAMS Fight Against Human Trafficking Committee*, a cause she holds dear to her heart, which develops employee volunteer programs and collaborates with organizations worldwide to assist in the fight against this heinous crime.

Prior to joining ACAMS, Montoya held over 15 years in strategic management for a wide range of corporations, industries and governmental organizations. Montoya holds a master's degree in international affairs from Florida State University and a bachelor's degree in international relations from Florida International University.

***ACAMS Today:* How has the ACAMS Risk Assessment tool evolved since its launch in December 2014?**

Tanya Montoya: The tool was developed with the basis that its evolution would depend on three major factors: global authoritative guidance and regulatory updates, subject-matter expert and user feedback, and cybersecurity protocols and best practices. Since the launch, we have kept our promise by staying abreast of the latest global guidance and regulatory updates and by making enhancements accordingly. From updating our country risk rating at least three times a year in line with the Financial Action Task Force's plenary sessions to launching our securities module in September 2016 to meet the AML risk assessment needs of the securities financial segment worldwide. Our latest addition, launched this summer, is a full suspicious activity report assessment category developed to support the needs of institutions looking to risk rate their internal controls.

AT: *What was the biggest challenge when building the product from its inception to its launch?*

TM: I would say that our biggest challenge became our biggest strength. With the support of our advisory board and John J. Byrne at the helm, we understood the importance of ensuring the standards set by the tool were truly global in nature. This meant our product development and launch schedule would be longer and require more extensive reviews and consensus than if we had based the content solely on U.S. guidance and regulation. Our commitment to setting global standards has paid off in that we are able to reach all regions with our offering. In the end, the fight against financial crimes is a worldwide endeavor and it is an honor for ACAMS to be able to support a financial institution's efforts in mitigating risk no matter the jurisdiction.

AT: *What is your favorite component of the software and why?*

TM: I would say more than any particular feature or benefit, it is our relationship with our users and the AML community at large that is at the top of my list. We have a user group that meets about three times a year, where I, along with Jeremy Thompson, our technical program manager, and Dr. Richard Harms, our lead subject-matter expert, have the unique opportunity to receive direct feedback that is used back at the home office for future product roadmapping. In between meetings, our open door policy with everyone using the application has benefited both parties immensely. Likewise, working with both the institutions and global regulatory bodies has afforded the risk assessment team with a priceless opportunity to keep working toward meeting our vision of offering institutions worldwide a standardized means of measuring, understanding and explaining their money laundering risks.

AT: ***As a longtime advocate for human trafficking (HT) awareness, can you tell us how you first became involved in fighting this heinous crime?***

TM: Raised in Colombia, South America, I remember at 15-16 years old, seeing many girls my age going overseas with the promise of legitimate job placements that would enable them to help their families back home. Soon after, we learned of their true fate and it became "the elephant in the room" at many social gatherings. The silence on this started to become deafening to me. Later on as an adult, I decided to conduct research on the subject, and it was Nicholas Kristof's book *Half the Sky* that paved the road for me to do more to break the silence.

AT: ***Tell us more about what the ACAMS Fight Against Human Trafficking Committee is currently doing to help fight HT?***

TM: We have three main objectives: awareness, community engagement and strategic collaboration to make a global impact. Currently, as Polaris Freedom Circle members, we are helping disseminate their most recent report, "The Typology of Modern Slavery" to our members. We are also supporting Kristi House, a local organization in Miami, Florida in their efforts as well.

AT: ***As an avid reader, what book are you currently reading?***

TM: I'm reading two actually: *Option B* by Sheryl Sandberg and Adam Grant, and *The Circle* by Dave Eggers.

Interviewed by: Alexa Serrano, CAMS, editorial assistant, ACAMS, Miami, FL, USA, aserrano@acams.org

QUIZ

Test your AML/CTF knowledge today!

Visit ACAMSToday.org to take the latest quiz

1. Which of the following is an example of a false positive?

A) A customer is falsely labeled as a risk
B) A customer gives false information to the FI
C) A customer or suspicious activity is overlooked as a risk
D) None of the above

2. Which conduit do cybercriminals use to move their funds?

A) Digital currency
B) Money mules and shell corporations
C) Money transfer services
D) All of the above

3. IP addresses are generally associated with an individual user, but they may or may not be associated with a specific computer or server.

A) True
B) False

QUIZ

ADVANCED CERTIFICATION GRADUATES

CAMS AUDIT

Cyprus

Georgia Zacharoudes, CAMS-Audit

Jordan

Ahmad Maher Abu Ali, CAMS-Audit
Mohammad Amer Abu Rahmeh, CAMS-Audit
Maraghrait Makhamreh, CAMS-Audit
Walid Mutaw'e Al-Tamimi, CAMS-Audit
Shereen Nasr, CAMS-Audit
Antone Sabella, CAMS-Audit
Ameen Sodqi Saleh, CAMS-Audit
Ahmad Darwish Tarteer, CAMS-Audit

Lebanon

Imad Habre, CAMS-Audit
Nadine Kambris, CAMS-Audit
Noha Makkook, CAMS-Audit
Ghada Roumanos Abou Jaoude, CAMS-Audit

Luxembourg

Giovanni Frau, CAMS-Audit

Qatar

Babita Balan, CAMS-Audit
Prasanna Haran, CAMS-Audit

Saudi Arabia

Salim Al Dabbagh, CAMS-Audit

United Kingdom

Mireille Moukarzel, CAMS-Audit
Margo Vakharia, CAMS-Audit
Varadarajan Viswanathan, CAMS-Audit

United States

Rosalind Griffie, CAMS-Audit

CAMS **GRADUATES**: MAY-JULY

Afghanistan

Nesar Ahmad Yosufzai

Albania

Hansi Latifi

Andorra

Maria Isabel Añor Casas
Marga Carrasco Escobar
Alejandro Carrillo Rodriguez
Andrea Cruz de Carrillo
Xavier Diaz Torres
Víctor Gay Martí
Victoria Mira Oliva
Enric Perarnau Peral
Maria Teresa Remon Bailon
Ricardo Rodriguez Fernandez
Maria Viota Maestre

Antigua and Barbuda

Rockell Harvey

Argentina

Maria Florencia Crespo
Gustavo Hernan Morell Segura
Gustavo Steiner

Aruba

Ramsay Acosta
Sharlene Croes
Gracienne Vasquez

Australia

Maxim Alves
Nicole Biskop
Chen-Hai Chang
Chi Chang Chen
Wei Jin Chien
Hung-Shi Chou
Joel Cook
Kun-Pao Fan Chiang
Mun Ting Fong
Timothy Hobbs
Po Hsiang Huang
Leigh Hunter
Cian Kivlehan
Chi Kwan Kong
Chun Yu Kuo
Wei Yeh Lee
Sumeer Pai
Bhaskara Potam
Mark Salinas
Amandeep Sidhu
Anastasia Simpson

Austria

Clemens Schweizer

Bahamas

Antoin Bowe
LaToya Dean
Jenell Sands
Annice Tucker

Bahrain

Khaled Al Alawi
Ajeet Dawani
Milind Divekar
Kogulan Kanesanathan
Khaled Nass
Saloni Prasad
Ashish Rawat
Rana Muhammad Usman Qamar

Bangladesh

Taher Ali
Muhammad Jahurul Haq
Muhammad Nazmul Hoq
Mohammad Hasan Imam
Muhammad Rejaul Islam
Md. Mahfuzul Hoque Talukder
Md. Rokon Uz Zaman

Barbados

Tricia Ellis
Vanessa Kodilinye

Belgium

Manuel Ghesquiere
Franck Mfonka
Damien Vanhaudenarde

Botswana

Thato Chalira

Brazil

Vinicius De Carvalho
Ronald Fast
Gilson Gonçalves
Vinícius Gonçalves
Bianca Gonzaga
Gabriela Mendes
Luiz Carlos Toscano Junior

British Virgin Islands

Ryan Best
Kadecia Harry

Cambodia

Wei Chi Wu

Canada

Oluyemisi Adeoye
Haleh Aghassi
Surelly Alcantara Tejera
Reaud Ally
Kolawole Banuso
Denise Barrett-Hubbard
Aline Baskalian
Meghan Becker
Lori Berg
Elvan Bilgic
Andrew Brushett
Kenroy Carr
Pascalle Castagne
Barbara Chan
Jeff Chan
Lindsay Chase
Farrah Ka-Yan Chow
Shae Chun
Sujin Chung
Jayson Coffield
Michael Crasto
Galiya Dairova
Mohamed Datoo
Jenessa DeYoung
Angela Dhak
Kelly Diaz Vivas
Maria Fabro
Steven Fantham
Michael Farzaneh
Fatema Fazal
Nicolas Fiorella
Nidhi Gaur
Marcio Gomes
Manvi Gor
Delecia Graham
Jason Harvey
Pan He
Timothy Heathcote
Brooke Horvath
Yen-Kai Hsiao
Christopher Hucalak
John Hui
Omer Husain
Amanda Hutchinson
Hussein Isingoma
Thomas Jackson
Julien Jones
Laurent Josso
Maria Amable Kallos
Sanjay Khanna
Apple Koo
Jeffrey Korolischuk
Pawel Kramarski
Vladimir Lahatski
Deodat Le
Doosoo Devin Lee
Queenie Lee
Shawn Leonard
Ka Ying Leung
Stephanie Leung
Chi Chu Liao
Sheri Macinnis
Martin Maglutac
Patrick Makembo
Emma Mangahas
Steven Marcus
Bruce Marshall
Nathalie Martineau
Yamna Martinez Vega
Mykhailo Matich
David L. Mendez Guarnizo
Ida Minaudo
Mariya Mirnaia
Abrar Mohar

Adrian Moscher
Sara Mucio
Aneeb Mughal
Johan Nicolle
Chantel O'Brien
Alexandra Orchard
Ashish Panjwani
Mariana Perez-Garcia
Nataliya Polyak
Cecilia Ramoutar
Carlos Heriberto Reyes Zelaya
Umraj Riarh
Amanda Rikhi
Rosemary Rutherford
Maria Saaghy
Michelle Sales
Ibrahim Shaalan
Hiral Shah
Rabeeya Siddiqui
Wing Kit Bryan Sin
Aqil Sivji
Milena Spiga
Michael Stahl
Velina Stankova
Gunawan Suherli
Jigar Thakkar
Matthew Thompson
Samia Trautvein
Elaine Trieu
Isaac Tsang
Sheldon Tse
Timothy Tse
Jean Tshim
Robert Tucci
Robert Uveges
Tracey Weeks
Hiu Tung Barbara Wong
Xingzhen (Joanne) Wu
Jay Yoon
Jing Si Zhuang

Cayman Islands

Dorleth Bodden
Lesley den Exter
Lavie Hobson
Michelle McLaughlin
Prudence Pryce
Rose Roberts

Chile

Ivonne Marcela Reyes Rojas
Mauricio San Miguel Vásquez

China

Mansoor Ali
Ping An
Beili Bai
Hao Bai
Jie Bao
Yintu Bao
Zheng Bian
Qian Cai
Shuang Cai
Yue Cai
Lin Cao
Luebo Cao
Ping Cao
Yi Cao
Min Chang
Yi-Ting Chang
Ying Che
Bingyan Chen
Huaidong Chen
Ivy Chen
Junheng Chen
Keyu Chen
Lixia Chen
Liying Chen
Mo Chen
Mofei Chen
Qian Yu Chen
Qiong Chen
Shouxin Chen
Simin Chen
Siying Chen
Taisheng Chen
Weitong Chen
Xiaohong Chen
Xinxin Chen
Xiu Chen
Yang Chen
Yanzhen Chen
Yichuan Chen
Yun Chen
Zhaorong Chen
Zhenhuan Chen
Beiyi Cheng
Hua Cheng
Lijuan Cheng
Shuang Cheng
Yan Cheng
Ming-Che Chou
Han Ching Chu
Lixin Cui
Weina Cui
Yajing Cui
Xiaoxia Deng
Mingzhu Deng
Xingyu Di
Hong Ding
Min Ding
Peng Ding
Rongrong Ding
Jing Dong
Junfeng Dong
Yaohua Dong
Yi Dong
Jinxin Du
Xinning Du
Yifei Du
Zehui Du
Sumei Fan
Tingting Fan
Yali Fan
Fei Fang
Hao Fang
Lishi Fang
Yongwei Fang
Dongliang Fei
Lanying Fei
Mei Feng
Qiaoyun Feng
Yu Feng
Zichao Feng
Lili Fu
Mengxia Fu
Jun Gang
Huating Gao
Yang Gao
Dongni Ge
Ning Geng
Kai Gong
Lei Gong
Xiaojian Gong
Joshua Gu
Qiuyi Gu
Jun Guan
Wanying Guan
Wenjing Guan
Yinyan Guan
Ziwen Guan
Wei Guo
Yan Guo
Yueming Guo
Yuhong Hai
Bing Han
Hua Han
Huizhe Han
Jialu Karen Han
Jie Han
Jing Han
Li Han
Tingyu Han
Qi Hao
Chu He
Jieqing He
Li Xia He
Meijian He
Xianghui He
Xiaoyan He
Yijin He
Yinglu He
Yuxiang He
Ying Chin Hsu
Jing Hu
Minghao Hu
Su Hu
Wentao Hu
Xuefei Hu
Ziwei Hu
Chi-Ming Huang
Chin Tsung Huang
Dachao Huang
Di Huang
Jieyi Huang
Jingya Huang
Lewen Huang
Mei Huang
Songjie Huang
Weibin Huang
Xia Huang
Xiaotong Huang
Xiaowen Huang
Zhi Huang
Hong Huo
Gaofei Ji
Jingyi Jia
Meng Jia
Ling Jiang
Xiangjun Jiang
Zhixing Jiang
Jiao Jiao
Rui Jiao
Chenyi Jin
Joe Jin
Tao Jin
Ryan Ke
Zhan Kuang
Hui Ru Lai
Wai Tat Lai
Zengqiang Lai
Jie Lan
Wenyan Lan
Xin Lei
Xiao Leng
Baocheng Li
Boyan Li
Feng Li
Guozhong Li
Haiyan Li
Hanyi Li
He Li
Huan Li
Hui Li
Huijuan Li
Huiling Li
Huiwen Li
Jing Li
Jun Li
Ke Li
Lisha Li
Meng Li
Menghua Li
Shao Li
Ting Li
Weihong Li
Wenlin Li
Xiao Li
Xiaolian Li
Xiaoling Li
Xiaolu Li
Xiaomei Li
Xiaoyan Li
Yangyang Li
Weitao Lian
Claudio Liang
Fangtao Liang
Sili Liang
Xiaoli Liang
Min Liao
Xia Liao
Yan Liao
Danliang Lin
Juan Lin
Lin Lin
Ling Lin
Shaolan Lin
Song Lin
Yang Lin
Yongbin Lin
Zen-Te Lin
Bo Liu
Chengyin Liu
Huiping Liu
Jian Liu
Kaiquan Liu
Li Liu
Ling Liu
Min Liu
Rong Liu
Shuai Liu
Xuemei Liu
Yanxia Liu
Yi Liu
Yingxia Liu
Zengjie Liu
Zengnan Liu
Ziyang Liu
Jialin Long
Peili Long
Hui Lu
Ming Tse Lu
Shimeng Lu
Xiaozhu Lu
Yehui Lu
Lu Lun
Bowen Luo
Chanjuan Luo
Fan Luo
Huaiyun Luo
Lixin Luo
Mei Luo
Yilan Luo
Yilong Luo
Yuzhen Luo
Zhankun Luo
Minyi Lv
Yican Lv
Haiyang Lyu
Wen Lyu
Jian Ma
Shaolei Ma
Wenlong Ma
Xiao Ma
Xiaorong Ma
Xinlin Ma
Yan Ma
Yongxin Ma
Chenxing Mao
Yajie Mao
Lei Meng
Xing Meng
Yi Min He
Meng Ni
Yifeng Ni
Min Nie
Wenqian Niu
Xin Ouyang
Hongxia Pan
Qian Pan
Chaoji Pang
Chunyan Pang
Jun Pei
Yan Pei
Zhaoyi Peng
Wenying Qi
Yang Qi
Xiangrong Qian
Jing Qin
Shuo Qin
Tiehong Qin
Ying Qin
Meng Qiu
Xiaoyi Qiu
Minxin Que
Yun Rao
Lanlan Ren
Fei Rong
Jie Shen
Jie Shen
Ruihong Shen
Wen Shen
Ting Shi
Zhenzhen Song
Yaotian Su
Hong Sun
Li Sun
Lihua Sun
Lin Sun
Yi Sun
Zhe Sun
Liu Tan
Wei Tan
Huan Tang

Xiaodong Tang
Dan Tao
Jing Tian
Ming Tian
Shan Tong
Yan Tong
Chaojing Wang
Chih Cheng Wang
Fang Wang
Ge Wang
Han Wang
Hongxia Wang
Hui Wang
Lina Wang
Lu Wang
Mingen Wang
Mingrui Wang
Pei Wang
Qiaoling Wang
Tian Wang
Yan Wang
Yanhong Wang
Yi Heidi Wang
Ying Wang
Yongchao Wang
Youhong Wang
Yuan Wang
Yuqi Wang
Yuqin Wang
Zonglian Wang
Hua Wei
Qin Wei
Daisy Ming Wen
Dujun Wen
Jianxia Wen
Xue Wen
Hongyan Wu
Jiebin Wu
Jingyun Wu
Ting Wu
Tong Wu
Wei Wu
Xiaojin Wu
Yicheng Wu
Zhenghua Wu
Zhimin Wu
Delin Xia
Xiaolan Xia
Xiaoyu Xia
Caixia Xiao
Han Xiao
Yajun Xiao
Yijie Xiao
Hong Xie
Luping Xie
Monique Xie
Qianru Xie
Li Xin
Bing Xiong
Tingting Xiong
Huisheng Xu
Jia Xu
Jiajia Xu
Lijuan Xu
Xiangdong Xu
Xin Xu
Zhenxing Xu
Bing Xue
Chen Xue
Jing Xue
Jun Yan

Pan Yan
Yiping Yan
Aaron Yang
Fan Yang
Huan Yang
Lei Yang
Lu Yang
Qian Yang
Rongdi Yang
Shuwei Yang
Weiling Yang
Wujin Yang
Zhengning Yang
Yiyu Yao
Chao Yin
Nan Yin
Fei Yu
Feijie Yu
Jie Yu
Tian Yu
Wei Yu
Weile Yuan
Yi Yuan
Hong Yun
Lixin Yun
Hao Zeng
Limin Zeng
Ling Zeng
Qingyu Zeng
Yanping Zeng
Zhibin Zeng
Zijian Zhai
Bin Zhang
Bo Zhang
Can Zhang
Chuojun Zhang
Dongyan Zhang
Haiyan Zhang
Heng Zhang
Herong Zhang
Heying Zhang
Huiyi Zhang
Lei Zhang
Liping Zhang
Minyang Zhang
Pei Zhang
Rongshan Zhang
Rui Zhang
Ruonan Zhang
Shuliang Zhang
Tong Zhang
Wanming Zhang
Weidong Zhang
Weiyi Zhang
Xi Zhang
Xia Zhang
Xiaodan Zhang
Xiaoyu Zhang
Yanmei Zhang
Yiting Zhang
Yiwen Zhang
Youzhi Zhang
Yuanyuan Zhang
Yue Zhang
Aiguo Zhao
Dongming Zhao
Guangquan Zhao
Jing Zhao
Jingsi Zhao
Lu Zhao
Sheng Zhao

Ting Zhao
Wenjun Zhao
Yan Zhao
Fei Zheng
Guolei Zheng
Haitao Zheng
Huimin Zheng
Jie Zheng
Li Zheng
Xiaoxue Zheng
Jianbin Zhong
Wenni Zhong
Yongmei Zhong
Zhenxin Zhong
Chunmei Zhou
Hao Zhou
Huijie Zhou
Jingwen Zhou
Qi Zhou
Wei Zhou
Yi Zhou
Yishan Zhou
Zhi Zhou
Linjing Zhu
Shaohua Zhu
Xiaolin Zhu
Xiaonan Zhu
Xiaoying Zhu
Yan Zhu
Hao Zou
Jia Kun Zou
Qian Zou
Qunrong Zou

Colombia

Carolina Hernández Hoyos

Costa Rica

Karen Chaves Calvo

Curaçao

Natasha Blomont
Christian Branum
Eugeline Cicilia
Jocelyn (Jocy) Croes
Marisol De Freitas Pereira
Ribella Dunker
Corinne Joubert
Anne-Marie Kemna
Miguela Lie Pauw Sam
Harold Pieters
Jean Rodriguez
Caroline Walraven

Cyprus

Aristos Aristidis
Sophie Ioannou
Tania Kyriakidou
Christina Michail
Lefkios Papadopoulos
Ekrem Seyman
Markos-Loukas Skoteinos
Andreas Sophroniou
Marcela Sramkova

Czech Republic

Pavel Matejka

Egypt

Eman A. Bakr Ahmed Mohamed

Estonia

Mait Kaselo

France

Julia Ablin
Grace Manuela Meliane Akpa
Patrice Bedikian
Jean Bouffard
Kuan Hua Chen
Jing Fong Chiou
Laurence Chirlias Harzo
Beatrice Collot
Monika Cwiertnia
Virginie Dorville
Olivier Cedric Dupont
Hafida El Issi
Pierre Fabre
Marie-Francoise Fevrier
Nathalie Freuchet
Nathalie Groll
Marielle Iaconelli
Allison Joie
Younes Khalifa
Wioletta Klasa
Sabine Leclerc
Virginie Leite
Philippe Meneguzzo
Eric Percheron
Clelia Ransford
Thierry Razanahoera
Renauld Roussette
Olga Thomas Semenova
Lucile Tolos
Wen Hsien Tsao
Samantha Vachez

Georgia

Alina Kvanchiani

Germany

Sandra Buschmann
Stefan Buxbaum
Christopher Entwistle
Nathalie Frank
Alexander Juettner
Tatyana Krym
Maren Neugebauer
Beate Poppe
Beate Prochaska
Katharina Stoll
Sascha Tangel
Jonathan Tridgell
Anna Tabea von Hein
Adrian Widera
Christoph Wronka

Ghana

Christian Amoakoh
Evans Andoh
Papa Ayiah
Esther Boahemah Antwi
Yvonne Botwe
Emil Meddy
David Nyanteh
Eunice Otoo

Greece

Saud Yassin

Guam

Eduardo Bernal

Guyana

Leon Anthony Belony

Honduras

German Rolando Lanza Giron

Hong Kong

Jiale An
Chien Kiat Ang
Fun Tat John Au
Sukanta Bag
Regan Catigbe
Brian Chan
Chloe Chan
Chung Yan Chan
Fu Ho Chan
Ka Shing Chan
Meilie Man Yee Chan
Mun Yi Chan
Pui Yee Chan
Shing Chan
Fu Chuan Chen
Hsin-Hung Chen
Dao Ming Jason Cheung
Josephine Wai Ying Cheung
Ernest Ka Leung Chiang
Chiung Chun Chien
Ling Cheong Anthony Chiu
Shuk Yee Chiu
Yuen Man Chiu
King Lung Cho
Hon Man Jacky Chong
Heiki Chow
Kin Chun Chow
Kwan-Lok Chun
Hiu Wai Chung
Hui-Lan Fan
Anita Fang
Robin Fine
Lai Yuen Fong
Martin Frieser
Yi Jun Fu
Chi Yu Fung
Kwan Ling Fung
Man Wai Fiona Fung
Indrani Ghosal
Nuot-Cla Giacometti
Chao Han
Ivan Yin Tat Ho
Ling Wai Ho
Siu Man Ho
Susanna Ho
Tiffany Hon
Chu-Li Hsiao
Su-Hui Hsu
Qing Hu
Michael Hui
Ka Wai Carl Hung
Yik San Hung
Yu-Ting Hung
Chung-Huey Hwang
In Young Hwang
Chung Wai Dominic Ip

Ka Ki Kenneth Ip
Kim Chun Ip
Rani Kamaruddin
Chi Ling Ko
Pui Yi Ko
Anthony Kumar
Ching Kong Kenneth Kwan
Ming Chiu Kwok
Hanson Yuen Yan Lam
Pak Nin Alam Lam
Shu Kit Lam
Garry Law
Vivian Che Yun Law
Grace (Ka Man) Lee
Hsin Chen Lee
Jessica Chieh Shi Lee
Eva Leung
Fiona Wing Yee Leung
Fung Yan Leung
Ka Wai Leung
King Yin Daniel Leung
Wing Yin Cowina Leung
Wing Yuen Leung
Ann Ying On Li
Man Chun Li
Man Hon Li
Shing Wa Li
Ting Wai Li
Wai Shan (Beatrice) Li
Yat Shan Catherine Lim
Dik Limbu
Yu-Tsung Lin
Shaoying Liu
Xiana Stephanie Liu
Cindy Shuk Yin Lo
Kit Wa Lui
Tsz Ying Silver Lui
Kwok Kuen Lung
Yat Nam Lung
Patrick Ma
Thomas Madden
Jenny Yim Fung Mak
Kit Yi Mak
Tsun Kit Andy Nam
Kai Ping Allen Ng
Veronica Ng
Yu Ho Ng
Kazuoki Okuma
Mei King Pang
Yeong-Wei Peng
Kannan Ravimohan
Pavandip Singh
Kwok Shun Geoff Siu
Chun Chung So
Mei Nga Sze
Rubie Tam
Yiu Tak Dickey Tam
Kam Ling Ting
See Ying To
Wai Ham To
Wing Hung Wan
Shuk-Ching Wang
Yung-Chi Wang
Paul Warhurst
Ching Ching Wong
Chun Kit Wong
Chun Lung Wong
Hang Yi Debby Wong
Hiu Tung Jacqueline Wong
Hoi Nam Wong
Wai Man Wong
Wilfred Tat Chee Wong
Wins Wong
Wai Woo
Fong Hiu Wu
Ka Ki Wu
Lok Yan Yau
Lok Yi Yeung
Ming Yeung
Sabina Wan-Ying Yeung
Yim Lan Yeung
Ka Man (Carman) Yu
Siu Hin Yu
Wei Chih Yu
Agnes Yuen
Kwok Keung Yuen
Wai Chun Yung
Chuanxiuxing (Daisy) Zhong

Hungary

Martyna Bojarska
Attila Szucs

India

Sonika Agarwal
Anurag Alleppa
U. Arumugamangalam
Ganesh Athreyaa
Vikram Babbar
Anjana Behera
Anuradha Bharadwaj
Vardharam Bhomaji Mali
Jyoti Chakrabortty
Somveer Chaudhry
Joydeep Chaudhury
Mohanraj Chellamuthu
Saurabh Chhabra
Wei Theng Chin
Suriyakumar C. Rajakumar
Snehal (John) Joseph D'Cunha
Swathy Devaraj
Shylessh Devarajan
Neha Dhamecha
Preeti Dokania
Sahil Gagneja
Aparna Garg
Rohit Garg
Gurbeer Gill
Madonna Gomez
Deepanshu Gulati
Keerthana Gunashekaran
Tarun Jain
Jemy Jose
Joseph Joy
Shweta Kamat
Bhanupriya Katira
Arushi Kaul
Mansi Keshri
Saurabh Khanna
Ravi Kumar Kudupudi
Amit Kumar
Ashutosh Kumar
Ashwin Kumar
Chetan Kumar
M J Bharat Vijay Kumar
Frida Macline
Maneesh Mathew
Sagar Mayte
Siddharth Mehrortra
Priyesh Mehta
Ruchira Mishra
Shashank Mohta
Manoj Mudaliar
Shahzia Mudbhatkal
Prasenjit Mukherjee
Ragavan Murali
Vinod Murali
Prakash Murthy
Chashveen K. G. Singh Nanda
Rakesh Nanda
Som Nanda
Jasbinder Neela
Suraj Padmanabhan
Malini Pagadala
Sabina Parween
Vikas Patil
Cletus Pereira
Kirupaakar Prakasam
Mohit Rawat
Selvaraj Santiago
Niranjan Satpathy
Gaurav Saxena
Vijay Anand Sekar
Abhishek Shah
Amrish Shah
Swathi Shekar
Vinit Shetty
Ambalika Shome
Anupama Singh
Kaushik Surendran
Dimple Thakkar
Ankush Thakur
Naveen Tiwari
Mayuree Vaseta
Mahalakshmi Veeramani
Narendra K. Venkatachalapathi
Murali Raj Vinayagam
Shruthi Vishwanath
Saroj Yadav

Indonesia

Mery Dwi Ambarukmi
Hani Kusumowardhani
Carina Melani
Nicodemus Pardede
Adinda Siahaan
Harris Simanjuntak
Nurul Yuniyanti

Ireland

Colm Dawson
Gavin Healy
Stefano Rossi
Rachel Sayegh

Israel

Hila Sion

Italy

Emmanuele Biroli

Jamaica

Gregory Simms

Japan

Hiromu Adachi
Yuki Enomoto
Hidekuni Fujioka
Eikichi Fukuzawa
Manabu Funayama
Ryosuke Hamagashira
Arisa Hasegawa
Minami Ishikawa
Shinya Izumi
Koji Kashimoto
Kenji Kobayashi
Naomi Kurahashi
Kensuke Morita
Aya Nakagawa
Hitoshi Nakao
Yuji Ono
Aleksandar Radosavljevic
Takayuki Saito
Yosuke Saito
Takashi Shimizu
Masaki Takahira
Kenichi Takakura
Emina Takashima (Tsuge)
Yuichi Takemura
Ryuichiro Tanabe
Chiyomi Tanaka
Hideo Tanaka
Kiyokazu Tanaka
Osamu Tobita
Tsung-Hao Tsai
Tsung Chih Wu
Yukihiro Yamamoto
Wakana Yokota
Hirokazu Yoshitake

Jordan

Ahmad Tayseer Abu Arab
Ahmad Abu-Alrob
Dina Ahmad Kreishan
Mohammad Ahmmad Bahboh
Omar Odeh Al Haj Mahmoud
Akram H. Waheeb Al Nidawi
Muath Rauf Al Qatnany
Rawand Zaid Alashram
Rasha Abdulelah Ali
Nada M.R. Al-Jabari
Mahmmoud Al-Jammal
Osama Issa Al-Salman
Nadeen Khalil Asfour
Eyad Bashar Ghanma
Amjad Raja Batayneh
Mustafa H. To'ma Al Mustafa
Ayham Nafez Hamadallah
Shihab Ahmed Hamdi
Mohammed S. Hameed AlSalim
Alia Hussam Almajali
Hadeel Azeez Kadhim
Hala Kayyali
Wael Mahmoud Alalami
Ahmad Marwan Jamous
Ahmad Mohammad Al Saidi
Nour Mohammad Al-Zaben
Hamzeh Mohammad Desh
Abdallah Mohammad Flaifel
Ameen M. Saeed AlFalah
Nahya Kadhim M. Al-Obaidi
Lubna Mohammed Suwan
Ali Fayez Nassif
Bushra Anwer Rashid
Bara Shafiq Al-Hihi
Wael Sweidan
Eman Waled Al Abdallat
Muath Wasef Salameh

Kenya

George Githaiga
Winnie Maina
Timothy Munene
Zachary Ochieng
Erica Wakisha

Kuwait

Dalal Abdul Salam AlSumait
Jassim Al-Hasawi
Abdulaziz Mustafa Haji Ali
Mohamed Kamel Farghal
Nassar Ghazi Al-Sheraian

Laos

Sisavad Chanthalangsy

Latvia

Zigmars Berzins
Inna Botmane
Olegs Druvietis
Alina Gamidova
Mihails Mohovs
Ksenija Novikova
Jevgenija Plotnikova
Jana Scerbaka
Natalja Tkachenko
Inese Zandava

Lebanon

Bassem Raja Al-Sayegh
Carine Chartouni
Amani Chedid
Nay Daaboul
Ali Hojeij
Rita Kabbabe
Layal Loutfi
Ali Makki
Nada Nakhoul
Saada Rahal
Bilal Saba Ayon
Pascale Semaan Mouanes
Kawthar Zantout

Lithuania

Gita Amsiejute

Luxembourg

Lisa Berschens
Sam Bopha
Mathias Emilsson
Céline Iammatteo
Carlota M. Andrada-Vanderwilde
Amélie Pfistner
Tobias Schnizler
Leonie Scott

Macau

Hong Ieng Chang
Ka Ieng Cheong
Sok In Stella Ian
Ka Man Iao
Kam Hou Ip
Liangxiang Kuang
Chi Hou David Lai
Cheng Kong Lam
Mui Iok Lam

Nicole Lam
Wai Kei Leong
Wai Kin Lo
Xianduo Meng
Quan Shi
Elizabeth So
Kin Ngai Tong
Kit Man Tse
Meizhen Xie
Duanduan Zhuang

Malawi

Susan Tengatenga

Malaysia

Nurhana Abd Rahman
Kathriya Ang
Huey Han Henry Ch'ng
Sue Ann Chua
Bernard Chuah
Geetha Ealangov
Sharanjeet Gill
Jo-Vyn Lai
Chih Shan Lee
Mohd Izwan Ali Mohd Long
Ali Asghar Salim
Devashini Satiananden
Ranjan Shahu
Dinakaran Sivalingam
Chin Xiong Tan
Mei Chee Yap

Malta

Daniela Attard Zerafa
Deborah Cassar
Antoinette Fenech
Charlotte Roberts

Mauritius

Joanne Albert
Vandana Boolell
Dharvish Chundydyal
Clotilde Domingue
Anusha Munisamy
Binsha Raderam
Anoop Ramroop
Avinash Seebhujun

Mexico

Erika Aguirre García
Jaime Daniel Del Rosal Calzada
Fernando Rafael Garcia Cuellar
Silvana García Pedrayes
Abhishek Khatri
Mario Alberto Maciel Castro
Aurea V. Martinez Fonseca
Raul Morelos Meza
Carlos M. Ramirez Rodriguez
Arturo Reyna Gaona
Alberto Rosiles Becerril
Jose Daniel Saldaña Sosa
Luis Alejandro Zarco Serrato

Monaco

Carole Pauselli

Morocco

Mohammed Aboutarik

Netherlands

Stefan Aalbers
Yasemin Bakker
Dennis Buunk
Yao Chien Chang
Yan de Bakker
Willem Maarten de Vos
Adrianna Fabijanska
Jiajia Gao
Anastasia Karydi
Rohini Nair
Aswien Oemrawsingh
Karen Schoorl
Jamey Ngan Shum Tang
Peter van Leeuwen

New Zealand

Sybrandt Botha
Andrew Grieve
Lisa Kerr
Hyeok Sang Lee
Maria Theresa Reyna

Nicaragua

Erwing Eleazar de Castilla Cisne

Nigeria

Solomon Abiakalam
Chukwudinma Okafor
John Olorundare
Adewale Olusesan Badejoko
Shofolahan Osho
Stephen Sanyaolu
Eric Tetegan
James Tomomewo

Oman

Alshaima Al-Shuaili

Pakistan

Naveed Rahman Atique
Shaukat Ali Bangash
Muhammad Moeenuddin
Irfan Qureshi
Muhammad Rais
Syed Ali Raza
Mohammed Riaz
Muhammad Usmani
Muhammad Waqas

Panama

Maria Angelina Belleza
Chia Hsiung Chen
Shih Kuan Chuang
Hui-Fen Kao

Peru

Patricia Valdiviezo

Philippines

Christian Emmanuelle Ang
Karyon Carreon
Lloyd Aldrin Dagdag
Alyanna Daphne Mabunga
Maria Isabelle Mandigma
Vicky Salas
Francis Sandro
Jill Priscila Santillan Soto
Kathleen Joy Taag

Poland

Shunsuke Araki
Marta Banaszczyk
Natalia Bieszczanin
Denitsa Blagova
Izabela Chrapicka-Gryzek
Tomasz Ciechonski
Malgorzata Czubaszek
Kaja Dembicka-Gur
Grzegorz Dmitruk
Rajesh Ganesan
Paulina Gozdek
Elzbieta Iwonin
Maciej Janas
Ewa Kizelbach
Anna Klik-Chylinska
Maciej Kolasa
Mateusz Koziel
Anna Krolikowska
Marcin Kulaga
Jakub Lewandowski
Paulina Lipska Azinger
Malgorzata Mackiewicz
Angelika Nowak
Maciej Przyslupski
Wiktor Rozanski
Miroslawa Rudnicka
Dominika Rudolf
Agata Skałba
Anna Szczepanik
Marta Tarczynska
Marcin Wasilewski
Ewelina Wegrowska
Robert Wojcik
Magdalena Wojtowicz
Shien Yi Loo

Portugal

Joao F. P. da C. Bargiel Pestana

Puerto Rico

Wendell Laracuente
Roberto Rodriguez
Luz Sullivan Rosado

Qatar

Delia Morna
Gayathri Ramadas
Marc Reaidi
Hongbo Sun
Saiful Vaidhyakkaran

Republic of Mauritius

Varinka Tandrayen

Russia

Andrey Nestrenko

Saint Kitts and Nevis

Kamilah Anderson-Rodgers
Neva Manners
Fayola Olugbala

Saint Vincent and the Grenadines

Kisha Sutherland

Samoa

Thomas Ah Yen
Naite Lolenese

Saudi Arabia

Muhanad Al Mutairi
Layla AlAraj
Norah Alharbi
Tamem Almajed
Abdullah Alowaini
Khalid AL-Qahtani
Meshan Mohammed Almeshal
Manoj Muliyil
Walaa Mushrf

Singapore

Divya Arun
Nishchint Baijal
Bedashruti Mitra Basu
Dominique Braun
Chi Wai Chan
Yang Chen
Limin Chow
Kelly Eng
Lim Foong Ming
Gerald Gan
Belinda Goh
Li Li Goh
Ling Ju Goh
Amanda Susan Gore
Sugandhi Govil
Aamir Hanif
Jesvin Kaur Harnak Singh
Muhammad Siddiq Ul Hassan
Hsia Lin Estee Ho
Jia Jing Ho
Jia Xin Ho
Whee Lang (Magdalene) Hoong
Ching Yi Hsiao
Zhimin Germaine Huang
Dhunjishaw Jagus
Anupam Jain
Anandhan Kannan
Carolien Kapel
Mehrunnisah Kasim
Joel Ker
Hong Yi Khoo
Li Lin Cheryl Khoo
Hwee Kiat Koh
Sok Jen Amy Kok
Tuck Fei Daniel Kong
Scott Lam
Pei Yang Lau
Regina Lee
Razel Legaspi
Cherie Lian
Tze Peen Liew
Denise Lim
Geok Juin Lim
Zhen Han Lim
Zhou Jin Kelvin Lim
Clifford Savio Lopez
Lina Mockeliunaite
Melvyn Mong
Subhasish Mukherjee
Veerappan Muthu
Thangaraja Nada Raja
Chay Liang Ng
Wan Yi Devonna Ng
Leire Nunez Cantero
Calvin Pang
Grace Wei Li Ping
Tharindu Prematillake
Ruo Yu Annette Qi
Ranjani Rangan
Supreeth Reddy
Rattanatham Rungwiteechaiporn
Viknesh Savagan
Elaine Seah
Saurabh Sharma
Michelle Shum
Sachin Bhanupratap Singh
Budiyanto Swatan
Ringo Takita
Angela Hui Min Tan
Chin Soon Benjamin Tan
Chuan Guan Tan
Elizabeth Shi Yu Tan
Li Lin Caroline Tan
Shanice Chew Hwa Tan
Tze Kee Toh
Choon-Boon Tok
Kun Chi Tsai
Rajkumar Vaikhari
Anand Vembaiyan
Melissa Wong
Wai Kit Wong
Marina Woon
Hung-Yi Wu
Elsie Yan
Jian Xiong Yang
Jiwu Yap
Siew Meng Yee
Zhi Rong Wilvia Yeo
Ho Youm
Wenjun Zhang
Kimi Zou

South Africa

Surekha Bhana Hiramaneck
Andries Breytenbach
Nirasha Chetty
Francois Combrinck
Marufu Dhakwa
Gary Jacobs
Rudi Kruger
Roama Manilal
Tshepo Moila
Jaco Nel
Inna Podsekina
Tabitha Ries

South Korea

Sa Rang Kang
Jangho Kim
Suk-Heon Kwon

Spain

Sadi Bezit
Rafael M. C. Gonbzalez De Anleo
Sergio Gallego Martinez
Estefanía García de Dios
Rebeca Gonzalez Santiago
Alvaro Gutierrez Gosalvez
Paula Grafulla González

Silvia Morando Fernández
Álvaro Pérez Ramón
Manuela Plotegher Arce
Ana Ramirez Medina
Carmen Maria Rascon Cordoba
Cristina Ruiz Sánchez
Lucia Suarez Barcia

Sri Lanka

Rajitha Fernando
Amani Udara Jayawardana
Annmarie Mendis
Seetharaman Muralidharan
Althaf Naseem
Induja Somasundaram

Sint Maarten

Bianca Bergsma

Switzerland

Fernando Jose Dyer Estrella
Hicham Hiddak
Jahanmehr Javaheri
Stefan Neumann
Ricardo Sánchez Plaza
Maria Lourdes Steiner
Nicholas Viggor

Taiwan

Yiun Bai
Mehng Ji Bau
Siang-Yao Cai
Zheng Ru Cai
Chia-Yu Chai
Chang-Hai Chan
Chih Hui Chan
Chih Wei Chan
Chin Yi Chan
Ching An Chan
Ching Chun Chan
Chu Ying Chan
Chun Yang Chan
Dan T.E. Chan
Erica Chan
Fei Ju Chan
Fu Chang Chan
Herman Ching Ho Chan
Kuei Lan Chan
Min Chi Chan
Shih Sheng Chan
Shu Ching Chan
Shu Min Chan
Shun Chuan Chan
Ya Hsuan Chan
Chao Kun Chang
Chen Chin Chang
Chen Wei Chang
Cheng Chiang Chang
Cheng Wei Chang
Chi Shun Chang
Chia Chen Chang
Chia Chi Chang
Chia Hao Chang
Chia Hua Chang
Chia Wen Chang
Chia-Chun Chang
Chia-Man Chang
Chia-Yin Chang
Chia-Yu Chang
Chih Hua Chang
Chih Ping Chang
Chih Wei Chang
Chih Yuan Chang
Chi-Hsiu Chang
Chin Chu Chang
Chin Fa Chang
Chin Lun Chang
Chin Wei Chang
Chin Yen Chang
Chin Yi Chang
Ching Yuan Chang
Ching Hui Chang
Ching Hung Chang
Ching I Chang
Ching Liang Chang
Ching Ting Chang
Ching Wei Chang
Ching Wen Chang
Chin-Hao Chang
Chuan Chuan Chang
Chun Mao Chang
Chun Ying Chang
Chung Chi Chang
Chung Wei Chang
Chun-Hsiang Chang
Fang Chi Chang
Fang Min Chang
Fu I Chang
Han-Bin Chang
Hsiang Yun Chang
Hsien Der Chang
Hsin Yu Chang
Hsinyun Chang
Hsiu Ping Chang
Hua-Shan Chang
Hui Ping Chang
Hui Yun Chang
Hui-Ling Chang
Jieh Kuen Chang
Kai Chieh Chang
Li Hui Chang
Li Syue Chang
Liang An Chang
Liang Chun Chang
Liang Wei Chang
Li-Fen Chang
Liling Chang
Ling Fang Chang
Lung Hsun Chang
Mei Hui Chang
Men Yu Chang
Meng Chung Chang
Min Chi Chang
Min Fang Chang
Min Liang Chang
Min Yi Chang
Ming Chun Chang
Ming Hsia Chang
Ming Yi Chang
Mu Chin Chang
Nai Yu Chang
Pei Chi Chang
Pei Lan Chang
Pei Lin Chang
Pei Wen Chang
Pei Yu Chang
Pi Chin Chang
Pi Chu Chang
Ruer Jan Chang
Shih-Fei Chang
Shiu Chin Chang
Shu Fen Chang
Shu Huei Chang
Shu Kwei Chang
Shu Ling Chang
Shu Mei Chang
Shu Ya Chang
Shu Yi Chang
Sophia Yu Ting Chang
Steven Chang
Su Ling Chang
Ta Chih Chang
Tian Shuen Chang
Tien Wei Chang
Ting Wei Chang
Tsao Lu Chang
Tsuey Ping Chang
Tsui Wen Chang
Tung Wei Chang
Tung-Yang Chang
Tzy Shin Chang
Wan Ya Chang
Wei Fen Chang
Wei Hung Chang
Wei Kuo Chang
Wei Wei Chang
Wei-Chang Chang
Wei-Ching Chang
Wen Chi Chang
Wen Hao Chang
Wen Hsing Chang
Wen Shin Chang
Wen Shing Chang
Wenting Chang
Ya Chen Chang
Ya Chu Chang
Ya Lun Chang
Ya Ting Chang
Ya Yun Chang
Yao-Hsin Chang
Yen San Chang
Yen-Lan Chang
Yi Chia Chang
Yi Chien Chang
Yi Ching Chang
Yih Cherng Chang
Yin Yin Chang
Yi-Yuan Chang
Yow Chyuan Jason Chang
Yu Chih Chang
Yu Fang Chang
Yu Hsien Chang
Yu Li Chang
Yu Shan Alice Chang
Yueh Hong Chang
Yu-Hsuan Chang
Yulin Chang
Yung Chi Chang
Yung-Tsung Chang
Yu-Ting Chang
Huan Yu Chang Chien
Yi Chia Chang Liao
Chih Yao Chao
Chin Yi Chao
Chi-Yuan Chao
Hsin-Jen Chao
Hui-Ju Chao
Hung Cha Chao
Mei-Ju Chao
Min Hsiu Chao
Shang-Chuan Chao
Wei Peng Allen Chao
Ya Hui Chao
Yi Jen Chao
Yu Chu Chao
Hsiang Cheng Che
An Lin Chen
An Ling Chen
Bo-Chun Chen
Bonnie Chen
Brigit Chen
Chang Sheng Chen
Chang-Tzu Chen
Chao Liang Chen
Chen Ling Chen
Chen Yang Chen
Chen Yang Chen
Chen Yu Chen
Chen-Jui Chen
Chen-Yu Chen
Chi Fang Chen
Chia Chiao Chen
Chia Chun Chen
Chia Hsiung Chen
Chia Ping Chen
Chia Yi Chen
Chi-An Chen
Chiang Hsin Chen
Chiao Hsin Chen
Chien Chih Chen
Chien Hsun Chen
Chien Hung Chen
Chien Liang Chen
Chien Lin Chen
Chien Ming Chen
Chien-Lun Chen
Chih Cheng Chen
Chih Hung Chen
Chih Ming Chen
Chih Shin Chen
Chih Yu Chen
Chin Chen
Chin Shiang Chen
Ching Chia Chen
Ching Ching Chen
Ching Han Chen
Ching Ho Chen
Ching Hung Chen
Ching Pei Chen
Ching Wen Chen
Ching Yi Chen
Ching-Shui Chen
Chiu Lan Chen
Chiu Yen Chen
Chun En Chen
Chun Hsiang Chen
Chun Kai Chen
Chun Liang Chen
Chung Hei Chen
Chung Wei Chen
Chun-Ling Chen
Chun-Yuan Chen
En Yu Chen
Fang Jung Chen
Fen Chen Chen
Feng Ru Chen
Feng Wen Chen
Fu-Yung Chen
Han-Yun Chen
Heng Chung Chen
Hsi Jung Chen
Hsiang Chu Chen
Hsiang I Chen
Hsiang Lan Chen
Hsiang Pin Chen
Hsiang-Hua Chen
Hsiao Hui Chen
Hsiao Yun Chen
Hsiao-Ting Chen
Hsien Cheng Chen
Hsin Wei Chen
Hsin Yen Chen
Hsin Yi (Portia) Chen
Hsing Chih Peter Chen
Hsing Ting Chen
Hsin-Hui Chen
Hsiu Chen Chen
Hsiu Chih Chen
Hsiu Hsien Chen
Hsiu Hui Chen
Hsiu Wen Chen
Hsi-Yuan Chen
Hsuan Chen
Hsuan Jung Chen
Hsuan Yu Chen
Hsuan-Yi Chen
Hsueh Chun Chen
Hsueh Ni Chen
Hsu-Han Chen
Huang Ren Chen
Huei Jen Chen
Huei Ling Chen
Hui-Ting Chen
Hung Chia Chen
Hung Ching Chen
Hung Te Chen
Hung Wen Chen
Hung-Yu Chen
I Chun Chen
I Hsuan Chen
I-Chun Sandy Chen
I-Fang Chen
I-Fu Chen
I-Hsin Chen
Ing Lin Chen
I-Pei Chen
I-Wen Chen
Jack Chen
Jaw Chen Chen
Jia Hui Chen
Jian Han Chen
Jui Jen Chen
Jui Sheng Chen
Jun-Dar Chen
Jung Chin Chen
Jung Chun Chen
Juy Choue Chen
Jyh Jye Chen
Kai Yin Chen
Kai-Hsiang Chen
Ko Hsin Chen
Kuan Ting Chen
Kuan Yen Chen
Kuei Chin Chen
Kun I Chen
Kun Sheng Chen
Kuo Hua Chen
Li Chin Chen
Li Hung Chen
Li Jang Chen
Li Jhou Chen
Li Jie Chen
Li Jung Chen

Li Wen Chen
Li Ying Chen
Li Yun Chen
Liang-Yin Chen
Li-Ju Chen
Ling-Ying Chen
Mei Chien Chen
Mei Hsueh Chen
Mei Hui Chen
Mei Ling Chen
Mei Ru Chen
Mei Wen Chen
Mei Yan Chen
Mei Yu Chen
Mei-Hua Chen
Mei-Jing Chen
Mei-Miao Chen
Meng Ting Chen
Meng Wu Chen
Ming Che Chen
Ming Chih Chen
Ming Kun Chen
Ming Mei Chen
Mu Tzu Chen
Nan Hung Chen
Naomi Chen
Pao Min Chen
Pei Chen Chen
Pei Chun Chen
Pei Hsin Chen
Pei Hsuan Chen
Pei-Shan Chen
Pei-Yi Chen
Peng-Yi Chen
Pi Na Chen
Pin Chun Chen
Pin Jhen Chen
Pin Yu Chen
Pin-Yao Chen
Pi-Tien Chen
Po Hsun Chen
Polly Chen
Roger Chen
Shao Hua Chen
Shao Kun Chen
Shao Yu Chen
Shei May Chen
Sheng Chieh Chen
Sheng Hsien Chen
Shiaun Liang Chen
Shih Hsuan Randa Chen
Shih Ming Chen
Shih Wei Chen
Shiueying Chen
Shu Chin Chen
Shu Fen Chen
Shu Feng Chen
Shu Hui Chen
Shu Ting Chen
Shu Yuan Chen
Shygh Shyone Chen
Siao Mei Chen
Sou-Lien Chen
Ssu Wei Chen
Su Tien Chen
Suen Pann Chen
Sze Ying Chen
Szu Ting Chen
Szu Ying Chen
Szu-Ting Chen
Szu-Yu Chen

Ting Wei Chen
Ting Yin Chen
Ting Yu Chen
Tsai Chieh Chen
Tsai Chin Chen
Tsuei Ying Chen
Tsui-Wei Chen
Tsung Ching Chen
Tzu Han Chen
Tzu Hao Chen
Tzu Ting Chen
Tzu Ying Chen
Tzy Dai Chen
Wan Yi Vicky Chen
Wei Chung Chen
Wei Dung Chen
Wei Jen Chen
Wei Jhen Chen
Wei Ting Chen
Wei Tso Chen
Wei Xiang Chen
Wei-Chih Chen
Wen Chien Chen
Wen Chih Chen
Wen Ling Chen
Xiao Yun Chen
Ya Chi Chen
Ya Chun Chen
Ya Hui Chen
Ya Ling Chen
Ya Wen Chen
Ya Ying Chen
Ya-Hui Chen
Yan Ming Chen
Yan-shing Chen
Yao Chung Chen
Ya-Tsu Chen
Yen Chen
Yen Ling Chen
Yen-Chin Chen
Yi An Chen
Yi Chin Chen
Yi Chun Chen
Yi Fang Chen
Yi Hsuan Chen
Yi Ju Chen
Yi Jung Chen
Yi Ling Chen
Yi Wen Chen
Yi Yin Chen
Yi Ying Chen
Yi-Ju Chen
Yi-Ju Chen
Yin Hsi Chen
Yin Lan Chen
Yin Lin Chen
Ying Huei Chen
Ying Ling Chen
Ying Yu Chen
Yinghua Chen
Ying-Ju Chen
Yu Chang Chen
Yu Chi Chen
Yu Chia Chen
Yu Chieh Chen
Yu Hsin Chen
Yu Hwa Chen
Yu Ting Chen
Yu Wen Chen
Yu Yang Chen
Yu Yu Chen

Yuan Chi Chen
Yu-Chieh Chen
Yueh Chien Chen
Yuhao Chen
Yun Chi Chen
Yung Chang Chen
Yung Chieh Chen
Yung Chu Chen
Yung-Ching Chen
Yuwen Chen
Yu-Wen Chen
Zih You Chen
Zong Si Chen
Chang Cheng
Chao Kai Cheng
Che Chung Cheng
Chia Cheng
Chia Ling Cheng
Chiang Chuan Cheng
Chien Ching Cheng
Chien-Ling Cheng
Chih Hsien Cheng
Chih-Ting Cheng
Chin Chin Cheng
Chun Liang Cheng
Fang-Sheue Cheng
Feng Fang Cheng
Fu Yu Cheng
Hong Ming Cheng
Hsiao-Hsuan Cheng
Hsin Yuan Cheng
Hsin-Mei Cheng
Hsiu Chu Cheng
Hsiu Hsiang Cheng
Hsiu Mei Cheng
Hsuan-Chun Cheng
Hsueh Kuo Cheng
Huang-Yu Cheng
Kuei Fan Cheng
Ming En Cheng
Miyun Cheng
Pei Chuan Cheng
Pin Shou Cheng
Ru Chun Cheng
Shu Fen Cheng
Su Ting Cheng
Su Yun Cheng
Szu Yu Cheng
Ting-Fang Cheng
Tsan Chieh Cheng
Yi Fan Cheng
Yi Ping Cheng
Yi Wen Cheng
Yi-Chin Cheng
Ying Chieh Cheng
Yu Che Cheng
Yu Chen Cheng
Yu Lin Cheng
Yu Tse Cheng
Yueh Hung Cheng
Yueh Yun Cheng
Ching Tung Chi
Ching-Yao Chi
Hsiao Tzu Chi
Shu Ying Chi
Tsai-Li Chi
Wei An Chi
Yin Hua Chi
Hsieh Chia Jui
Li Kuen Chian
Chao Hung Chiang

Chui Pin Chiang
Chun Hung Chiang
Chun Yi Chiang
Chung Hsiang Chiang
Chung Lung Chiang
Fa Jen Chiang
Fang-Fang Chiang
Fu Tsung Chiang
Hsin Yi Chiang
Hsu Hui Chiang
Hui Chuan Chiang
Hui Wen Chiang
Jui Yu Chiang
Ling Hui Chiang
Ming Chen Chiang
Pin Yu Chiang
Su-Fen Chiang
Ting Chieh Chiang
Ting Ying Chiang
Ya Ting Chiang
Yi Chun Chiang
Yu Lien Chiang
Chang Chia-Sheng
Guey Fung Chiau
Chun-Hsia Chien
Chun-Hui Chien
Hsiang Hsuan Chien
Jung Chia Chien
Li Hua Chien
Li Shih Chien
Mei Hui Chien
Pei Ju Chien
Shu Li Chien
Tsai Ta Chien
Tsai Ying Chien
Wan-Yin Chien
Wen Nan Chien
Ya Chu Chien
Yu Lung Chien
Cheng Chih Chih
Lin Chih Heng
Chih Chung Chin
Li Heng Chin
Pei Hua Chin
Chang Ching-Yi
Lih-Hwang Chiou
Sheue Ling Chiou
Chao Yu Chiu
Cheng Hao Chiu
Chung Ching Chiu
Hsin Ying Chiu
Huan Hsiang Chiu
Hung Chih Chiu
Kuan Kai Chiu
Kuo Min Chiu
Li Hua Chiu
Li Yang Chiu
Mei Ju Chiu
Po Hao Howard Chiu
Tsai Ping Chiu
Tsung Ming Chiu
Wei Lin Chiu
Wen-Ling Chiu
Yi Hsuan Chiu
Ying Chiu
Yu Ching Chiu
Yu Ya Chiu
Yueh Chin Chiu
Yu-Mei Chiu
Hsiao Jung Cho
Hsin Yi Cho

Hui In Cho
Jung San Cho
Ling Yu Cho
Ming Hung Cho
Shu Chuan Cho
Yin Wen Cho
Chen Yu Chou
Chi Yu Chou
Chia Pei Chou
Chia Yeh Chou
Chia-Hui Chou
Chih Ying Chou
Chin-Hui Chou
Fong Yi Chou
Hsiu Chen Chou
Hui Ting Chou
Hui-Chen Chou
Hung Chih Chou
Hung Chun Chou
Jing Lan Chou
Mei Lan Chou
Mei Rong Chou
Min Chen Chou
Min Chims Chou
Mou Hsing Chou
Nien-Yung Chou
Ronald Bo Yin Chou
Shan-Lin Chou
Shu Ping Chou
Te Chin Chou
Wan Chun Chou
Wan Lin Chou
Wei Yi Chou
Wen Jen Chou
Ya-Yun Chou
Yen Ju Chou
Yi Chi Chou
Yi Chien Chou
Yi Ru Chou
Yuan-Fang Chou
Chun Chiang Chu
Chung Tai Robert Chu
Chun-Hui Chu
Hsiao Chung Chu
Hsiu Lan Chu
Hung Yun Chu
I Chia Chu
Li Hua Chu
Shih Jen Chu
Tzuhsien Chu
Yi Cheng Chu
Yi Ping Chu
Yo Seng Chu
Yu Lien Chu
Chao Tsung Chuang
Chin Hsiu Chuang
Fei Ping Chuang
Hsueh Fang Chuang
Hsueh-Hui Chuang
Hui Yu Chuang
Huifen Chuang
I Ting Chuang
Li Shuang Chuang
Mao Yin Chuang
Meng Tsang Chuang
Po Chih Chuang
Rui-Ling Chuang
Shan Chi Chuang
Shiou-Ling Chuang
Shu Fen Chuang
Shu Yu Chuang

Te Hung Chuang
Ti Yuan Chuang
Wanchi Chuang
Ya Lan Chuang
Yi Heng Chuang
Yu Fang Chuang
Yu Ting Chuang
Huang Yu Chuang Lin
Chie Sheng Chueh
Wen Ling Chui
Pan Chun Liang
Chia-Chi Chung
Chiao Ling Chung
Chia-Wei Chung
Chih Feng Chung
Chih Hui Chung
Ching Fang Chung
Ching Feng Chung
Chun Yi Chung
Hsin Ju Chung
Hsin-Yi Chung
Hwa Guang Chung
Jui Shiung Chung
Li Ting Chung
Pei Yun Chung
Ping Yang Chung
Po Ting Chung
Shiang Lian Chung
Shih Chun Chung
Tsai Hua Chung
Tsai Ling Chung
Wen Ku Chung
Yi Chi Chung
Lin Chung Yuan
Lih Kan Chuo
Tsung Han Chuo
Jen Jen Chyr
Yu Chi Deng
Jia Chyi Ding
Pei Lin Dong
Ren Jye Duann
Chia Lun Fan
Chiao-Ju Fan
Chieh Min Fan
Chien Yuan Fan
Li Hsin Fan
Su Jung Fan
Ching-Szu Fang
Hsiang Jung Fang
Kuei Li Fang
Lan Hsin Fang
Wan Yin Fang
Yi Ting Fang
Yung Ming Fang
Chieh Feng
Pan Ching Feng
Yuh Li Feng
Chi Yen Fu
Chiang Fu
Chih Min Fu
Shih Ting Fu
Shu Chen Fu
Shu Ya Fu
Yu Chen Fu
Jhih-Han Gao
Jau Chyong Gau
Lih-Jen Goong
Hwei-Ju Guo
Yi Chun Guo
Yi Ying Guo
Pin Lun Han

Shu Ting Han
Tsung Tao Han
Wen Han
Chi Ting Haung
Hsiang Yen He
Pei-Wen He
Chao An Ho
Chi Fang Ho
Chia Hui Ho
Chun Chieh Ho
Chun Te Ho
Chun-Chen Ho
Hsin Yi Ho
Hui Chen Ho
Jia Jing Ho
Ju- Hui Ho
Kun Lin Ho
Lan Fen Ho
Pan Chung Ho
Pei Ju Ho
Pin Shiuan Ho
Pin-Chueh Ho
Po Ting Ho
Ssuwei Ho
Wei Hsiang Ho
Yin Hsiang Ho
Chia I Hong
Jialin Hong
Rong Liang Hong
Ruo-Cheng Hong
Siao Ting Hong
Shan-Min Horng
Chia Ming Hou
Chun Yi Hou
Hsiu Yu Hou
Liang Yu Hou
Ting Tzong Hou
Wen Liang Hou
Jie-Yun Hsia
Chia Ling Hsiao
Ching Fang Hsiao
Chiu-Feng Hsiao
Fang Yu Hsiao
Grace Hsiao
Han-Yun Hsiao
Hsiang Chun Hsiao
Hsin Yu Hsiao
Hsuan Hsiao
I Chen Hsiao
I Tien Hsiao
Kuan Chun Hsiao
Kuang Jung Hsiao
Kuei Tan Hsiao
Mao Hung Hsiao
Mei-Hua Hsiao
Mi Hsiao
Ming-Tsung Hsiao
Pei Hsin Hsiao
Ya Ling Hsiao
Yu Chieh Hsiao
Yu Hua Hsiao
Yu Jhen Hsiao
Yu Shun Hsiao
Sen Hsien Hsiau
Cheng-Chou Hsieh
Cheng-Chuan Hsieh
Chi Ying Hsieh
Chia Ming Hsieh
Chieh Ling Hsieh
Chih-An Hsieh
Ching-Cheng Hsieh

Chiu Mei Hsieh
Chuan Chih Hsieh
Chuan-Teng Hsieh
Elaine Hsieh
Fu Ju Hsieh
Hsiao Ching Hsieh
Hsiao Ling Hsieh
Hsin Chien Hsieh
Hui Wen Hsieh
Hui Wen Hsieh
Hui-Mei Hsieh
Jung Kuei Hsieh
Kuen-Ru Hsieh
Kun Wang Hsieh
Li Wei Hsieh
Ming Han Hsieh
Ming Kun Hsieh
Ming Yu Hsieh
Ming Yun Hsieh
Pei Chien Hsieh
Ping Fu Hsieh
Po-Ting Hsieh
Shu Fen Hsieh
Shu Yueh Hsieh
Su Hua Hsieh
Su Lin Hsieh
Su-Chen Hsieh
Tsu Fen Hsieh
Tsung Chi Hsieh
Wen Hao Hsieh
Ya Wen Hsieh
Yao-Chung Hsieh
Yi Chun Hsieh
Yi Ting Hsieh
Yi-Na Hsieh
Hsiu Chin Hsin
Yung Teng Hsin
Hsien-Tzu Hsing
Kuang Jen Hsing
Kuma Hsiung
Wan Jou Hsiung
Che Ming Hsu
Chen Hong Hsu
Cheng-Jui Hsu
Chen-Ling Hsu
Chi Han Hsu
Chia Chi Hsu
Chia Fen Hsu
Chia Ju Hsu
Chia Kuo Hsu
Chih Pin Hsu
Chih Yuan Hsu
Chin Chang Hsu
Chin Yi Hsu
Ching Ching Hsu
Chiu Feng Hsu
Chiung Chin Hsu
Chun-Chi Hsu
Fang Yu Hsu
Fang-Kuei Hsu
Fu Lung Hsu
Fu Yang Hsu
Hao En Hsu
Hau Tze Hsu
Ho Cheng Hsu
Hsiao-Jen Hsu
Hsin Fang Hsu
Hsin Yi Hsu
Hsin Yu Hsu
Hsinying Hsu
Hsiu Li Hsu

Hsiu-Feng Hsu
Hsu Tai Hsu
Hui Ling Hsu
Huiju Hsu
Hung-Hao Hsu
Jui Han Hsu
Jui Ying Hsu
Kai Ping Hsu
Kuo Che Hsu
Kuo-Cheng Hsu
Li-Hua Hsu
Lishin Hsu
Mei Chih Hsu
Mei Hui Hsu
Mei Shan Hsu
Meng Li Hsu
Min Lang Hsu
Ming Hsiu Hsu
Ming Yao Hsu
Pei Jun Hsu
Peter Hsu
Pi Chuan Hsu
Pi Yi Hsu
Ruey Wen Hsu
Shih Hung Hsu
Shih Yu Hsu
Shu Fong Hsu
Shu Lin Hsu
Shu Mei Hsu
Shu Neng Hsu
Sin Chung Hsu
Su Yu Hsu
Sung Chuan Hsu
Ta Kai Hsu
Tien Chin Hsu
Ting Hsu
Tsang Huai Hsu
Tsung Min Hsu
Tzu Fang Hsu
Wan Chi Hsu
Wan-Ting Hsu
Wei Hsu
Wei Che Hsu
Wei Chen Hsu
Wei Hsiu Hsu
Wei Lin Hsu
Wen Chung Hsu
Wen I Hsu
Wen Lan Hsu
Yao Wen Hsu
Yeh Chung Hsu
Yi Ling Hsu
Yi Wen Hsu
Ying Shuang Hsu
Yu Chieh Hsu
Yu Fang Hsu
Yu Hsueh Hsu
Yu Ting Hsu
Yuching Hsu
Yueh Lin Hsu
Yun-Chen Hsu
Yu-Wen Hsu
Bi Chih Hsueh
Cheng Fang Hsueh
Chiao Ni Hsueh
I-Ling Hsueh
Po Wen Hsueh
Sheng Ping Hsueh
Shiow Jeng Hsueh
Ya Chin Hsueh
Ya Yun Hsueh

Yu Wen Hsueh
Ching Cheng Hu
En Chia Hu
En Heng Hu
Fu Sen Hu
Heng Chin Hu
Hsueh-Sheng Hu
Huey Jyh Hu
Hui-Tzu Hu
Jia Huei Hu
Jia Rong Hu
Tzu-Yi Hu
Wan Ching Hu
Wei Hao Hu
Ya Ping Hu
Yu Ru Hu
Hsiang Lan Hua
Lei Hua
Su Huan Chun
Bor Shiun Huang
Chen Ling Huang
Cheng An Huang
Cheng Chou Huang
Chi Hsien Huang
Chi Wei Huang
Chia Hua Huang
Chiayen Huang
Chichao Huang
Chien Fu Huang
Chien Hao Huang
Chien Hsun Huang
Chien-Lin Huang
Chih Chi Huang
Chih Chieh Huang
Chih Sung Huang
Chih Wei Alan Huang
Chih-Yuan Huang
Ching Han Huang
Ching Ling Huang
Ching Yao Huang
Chi-Rong Huang
Chiu Hsia Huang
Chiung Yu Huang
Chong-Ming Huang
Chu Kuang Huang
Chuan Yuan Huang
Chun Cheng Huang
Chun Wei Huang
Chung Yi Huang
Chun-Ta Huang
Fei Huei Huang
Fu Jou Huang
Hsiao Hui Huang
Hsiao Wen Huang
Hsin Chieh Huang
Hsin Pao Huang
Hsin-Pei Huang
Hsiu Mei Huang
Huan Chang Huang
Hui Ching Huang
Hui Yuan Huang
Jang Chih Huang
Jing-Chou Huang
Jui Cheng Huang
Jun Kai Huang
Kai Chun Huang
Kuan Ying Huang
Kuo Wei Huang
Li Ching Huang
Li Hua Huang
Li Ling Huang

Li Ting Huang
Lien Sheng Huang
Lynn Huang
Mei Chi Huang
Mei Hui Huang
Mei Lan Huang
Mei Yu Huang
Meihui Huang
Min Hua Huang
Ming Chuan Huang
Ming Hsien Huang
Ming Ji Huang
Nien-Sui Huang
Pao Sung Huang
Pei Ching Huang
Pei Chun Huang
Pinghsi Huang
Po Kan Huang
Sheng Chieh Huang
Shih Min Huang
Shih Yuan Huang
Shu Chuan Huang
Shu Er Huang
Shu Fen Huang
Shu Hua Huang
Shu Ling Huang
Shu Min Huang
Shu Yun Huang
Shwu Jiuan Huang
Shwu Lih Huang
Siang Wei Huang
Ssu I Huang
Tai Chen Kyle Huang
Tang-Yueh Huang
Te Chang Huang
Tien Chen Huang
Ting Ying Huang
Tsanyi Huang
Tsung-Pin Huang
Tzu Lung Huang
Wan Chi Huang
Wan Ching Huang
Wan Hsin Huang
Wan Ting Huang
Wan-Ling Huang
Wei Hua Huang
Wei Yi Huang
Wen Hui Huang
Wen Jeng Huang
Wen Syuan Huang
Woei Tyng Huang
Ya Lan Huang
Ya Li Huang
Ya Ling Huang
Ya-Hui (Arial) Huang
Yalun Huang
Yen Fen Huang
Yen Hsin Huang
Yi Fan Huang
Yi Wen Huang
Yi Yin Huang
Yichun Huang
Yiwen Huang
Yu Chien Huang
Yu Ching Huang
Yu Hsiang Huang
Yu Lun Huang
Yu Shan Huang
Yu Ting Huang
Yu-Chun Huang
Yueh Feng Huang

Yun Chieh Huang
Yun Lan Huang
Yung Chen Huang
Yung Chuan Huang
Yu-Sin Huang
Chao Huang Hung
Chen Hwei Hung
Cheng Chan Hung
Cheng-Wei Hung
Chi Hsia Hung
Chi Yu Hung
Chia Heng Hung
Chien Hsin Hung
Chien Yu Hung
Chin Yuan Hung
Chin Jui Hung
Ching Chou Hung
Ching-Hsia Hung
Ching-Hua Hung
Hsuan Hung
Hui Chun Hung
Huichi Hung
Jui Sheng Hung
Jui Yang Hung
Jung-Chen Hung
Kuo Hsiang Hung
Ling Yi Hung
Man Chun Hung
Mei Ju Hung
Mei Ling Hung
Shu Ya Hung
Su Chen Hung
Su Yan Hung
Te Fang Hung
Tzuwei Hung
Wei Yu Hung
Wen Chieh Hung
Wen-Jiaw Hung
Yao Chao Hung
Yi-Hsiung Hung
Ying Shan Hung
Yu Chian Hung
Yu Chieh Hung
Yu Han Hung
Yu Ting Hung
bao jyh Hwang
I Ching Hwang
Meei Chwen Hwang
Shu Min Hwang
Yu Sheng Hwang
Ching Yen Jan
Hui Jiuan Jan
Yung Sung Jan
Wen Lih Jang
Chi Jen Yin
Yih-Sheng Jeng
Huei Sia Jhang
Borong Jheng
Yi Jiie Jhou
Ci-Chung Jhuo
Yimei Jian
Jing Long Jiang
Pei Yi Jiang
Sin-Huei Jiang
Wei Ting Jiang
Wen Sheng Jiang
Yu-May Jiang
Sin-Hong Jou
Wen Huei Jou
Jau Yin Ju
Shiow-Chyn Ju

Hsin Ying Juan
Ting Yen Juan
Chwen Ling Juang
Mei-Jun Juang
Mao-Chi Jung
Yi Ru Juo
Liou Yinn Jwo
Hsiu Jung Kan
Chin Chi Kang
Fu Chieh Kang
Fu Jen Kang
Hui Ju Kang
Jui Ying Kang
Jung Ching Kang
Shu Wen Kang
Being Tyzer Kao
Chi Yuan Kao
Chien Hua Kao
Chih Hui Kao
Kai-Pin Kao
Kan Tao Kao
Lee Hsueh Kao
Li Chih Kao
Li Wen Kao
Mei Li Kao
Sheng Yen Kao
Shu-Hui Kao
Su Yueh Kao
Su-Hua Kao
Tai Yin Kao
Ya Chen Kao
Yeh Sheng Kao
Yi Ying Kao
Ying Ying Kao
Yu-Ping Kao
Chun-Chih Ke
Jui Tang Ke
Peng-Zheng Ke
Wen Ting Ke
Tao Lin Keng
Chia Ying Ko
Chien Cheng Ko
Hui Chun Ko
Jou Yi Ko
Shu Hui Ko
Wei Jie Ko
Yao-Chun Ko
Yi-Lien Ko
Yung Fu Ko
Cheng Hung Ku
Li Chen Ku
Po Fu Ku
Mu-Lien Kuan
Nan Hung Kuan
Tzu Chen Kung
Chen Ming Kuo
Cheng Lin Kuo
Chia Yun Kuo
Chih Chun Kuo
Chih Ming Kuo
Chiu Mei Kuo
Chiu Yueh Kuo
Chun Lan Kuo
Emily Kuo
En-Wei Kuo
Fang Cheng Kuo
Hong-Chun Kuo
Hsien Shan Kuo
Hsiu Lin Kuo
Huai Hsiang Kuo
Huei-Ching Kuo

Huimei Kuo
Ing Jun Kuo
Li Yun Kuo
Meei Yue Kuo
Mei Hsiang Kuo
Meng Jen Kuo
Pai-Lan Kuo
Pusyuan Kuo
Shou-Ming Kuo
Shu-Huei Kuo
Su Chun Kuo
Tzu Ling Kuo
Wan Ting Kuo
Wen Liang Kuo
Wu Tsung Kuo
Ya Chin Kuo
Yen Ju Kuo
Yen-Han Kuo
Yi Chieh Kuo
Yi Ling Kuo
Yi Wen Kuo
Ying Chun Kuo
Yu Gean Kuo
Yu Hua Kuo
Yu-Lin Kuo
Yun Ting Kuo
Chao Ying Lai
Cheng Chang Lai
Chia Chi Lai
Chieh Ying Lai
Chien Chi Lai
Hsin Yi Lai
Hsiu Ling Lai
Hui Ching Lai
Hui Ni Lai
Hung Chi Lai
Hung Lin Lai
Hung Ta Lai
Jung Nan Lai
Kun Tang Lai
Len Lung Reynold Lai
Mei Ling Lai
Ming Hung Lai
Ming-Yan Lai
Pei Hsuan Lai
Pi Sheng Lai
Pin Chen Lai
Ru Yi Lai
Shu Ching Lai
Su Li Lai
Te Jen Lai
Tzung Pin Lai
Wanju Lai
Wen Chieh Lai
Wen Chou Lai
Wen Hsiung Lai
Yi Hui Lai
Yi Ping Lai
You Chi Lai
Yu Ning Lai
Yung An Lai
Chien Ming Lan
Pi Shang Lan
Ya Ling Lan Yi Fen Lan
Yu Chen Lan
Bing Kun Lee
Changhsien Lee
Cheng Hsien Lee
Cheng Lin Lee
Chi Jong Lee
Chi Wei Lee

Chia Hui Lee
Chia Ju Lee
Chia-Chun Lee
Chien Ming Lee
Chih Fang Emma Lee
Chih Hsin Lee
Chin Cheng Lee
Chin Yu Lee
Ching-Ching Lee
Ching-Chun Lee
Chun I Lee
Chun Jen Lee
Chun Ming Lee
Chun-Jen Lee
Hsiao Chuan Lee
Hsiao Han Lee
Hsien Hsiu Lee
Hsi-Lian Lee
Hsin Jen Lee
Hsin Yi Lee
Hsiu Hsia Lee
Hsueh Ping Lee
Hui Fang Lee
Hui Jung Lee
Hung-Chi Lee
I Chen Lee
Ing Ren Lee
I-Ting Lee
Jian Pyng Lee
Jinchich Lee
Kuang-Yu Lee
Kuo Hsien Lee
Kuo-Chi Lee
Li Min Lee
Lichiu Lee
Li-Ya Lee
Man-Chun Lee
Mei Hsiang Lee
Mei Yen Lee
Meng Ta Lee
Mi Chieh Lee
Ming Che Lee
Ming Fung Lee
Ming Kuang Lee
Ming Shan Lee
Pei Chia Lee
Pei Jung Lee
Pei Ling Lee
Pei Yu Lee
Pei-Ching Lee
Pin Shiow Lee
Po Ling Lee
Rou Hsien Lee
Shien Jen Lee
Shih Chiang Lee
Shirley Lee
Shu Kuan Lee
Shu Ting Lee
Shu Yi Lee
Shu-Fen Lee
Ssu Ying Lee
Sun Ho Lee
Sung Lin Lee
Tsung Sheng Lee
Tung Ying Lee
Tzu Yin Lee
Tzu Ying Lee
Wan Chen Lee
Wan Yu Lee
Wei Chen Lee
Wei Chieh Lee

Wei Yen Lee
Weishan Lee
Wen Chi Lee
Wen Hsing Lee
Wen-Bin Lee
Ya Wen Lee
Yao-Jung Lee
Ya-Yu Lee
Yen Ju Lee
Yi Fang Lee
Yi Fen Lee
Yi Hsuan Lee
Yi Hua Lee
Yi Ping Lee
Yi-Chun Lee
Yi-Jung Lee
Yu Ching Lee
Yu Hsiu Lee
Yu Ling Lee
Yu Ma Lee
Yuan Hua Lee
Yuhsin Lee
Yu-Hsuan Lee
Yu-ting Lee
Fu Cheng Lei
Ann Gane Li
Cai Yan Li
Che-Hua Li
Chen Yu Li
Cheng Hsien Li
Chi Ying Li
Chiao Chi Li
Chih-Chi Li
Ching Mei Li
Ching Shien Li
GuoHsien Li
He Yu Li
Hsing Chuan Li
Huan Chi Li
Hui-Ching Li
I Ni Li
Jhing Yu Li
Jui-Mei Li
Kang Yi Li
Meng Fang Li
Meng Yun Li
Ming Fang Li
Ming-Shiun Li
Pamela Jia Hang Li
Pei Chi Li
Pei Jung Li
Shih Wei Li
Syue-Ling Li
Ting Yi Li
Yi Chun Li
Yi Shian Li
Yu Chen Li
Yu Ching Li
Yueh Hua Li
Yun Ching Li
Yun Ju Li
Yun Pei Li
Yun-Bin Li
Yun-Mei Li
Cheng Hong Liang
Chia Ling Liang
Fang Yu Liang
Hsiu Chen Liang
Jyh Jong Liang
Li Ching Liang
Ling Ying Liang

Su Yu Liang
Wen-Yen Liang
Yi Kai Liang
Yuan Yi Liang
Yung Chen Liang
Chang Yuan Liao
Che-I Liao
Chi Hung Liao
Chia-Jen Liao
Chun Feng Liao
Chung Chieh Liao
Chung Hao Liao
Chung Yang Liao
De-Chung Liao
Fu Hsiang Liao
Hsiang Tai Liao
Hsiao Chun Liao
Hsien-Wei Liao
Hsin Ju Liao
Hsuan An Liao
Huei Min Liao
Kuo Hsiung Liao
Li Yun Liao
Ling-Ya Liao
Miao Jyuan Liao
Min Hsing Liao
Ming Kao Liao
Pei Chuan Liao
Pei Huang Liao
Pei Wen Liao
Shiue Chian Liao
Shu Fen Liao
Shu Hsun Liao
Shu Ju Liao
Shu Ming Liao
Shu Sia Liao
Shu-Chen Liao
Ting Hsuan Liao
Tzu Ya Liao
Wan Ting Liao
Wan-Ju Liao
Yi Chun Liao
Yi Ling Liao
Yi Ting Liao
Ying Ching Liao
Ying Ju Liao
Ying Ting Liao
Yueh Ying Liao
Yung Chao Liao
Vinci Liaw
Chih Ching Lien
Huei-Chi Lien
Hui-Ling Lien
Li-Chin Lien
Po Wei Lien
Yu-Hui Lien
Bing Hung Lin
Chao Chun Lin
Chao Ling Lin
Chao Tsung Lin
Chen Hui Lin
Chen Su Lin
Cheng Ta Lin
Cheng Yi Lin
Cheng Yih Lin
Cheng-Lung Lin
Chi Hao Lin
Chi Hsu Lin
Chi Sheng Lin
Chi Yen Lin
Chi Yi Lin

Chia Ching Lin
Chia Feng Lin
Chia Hsiang Lin
Chia Hua Lin
Chia Hung Lin
Chia Jung Lin
Chia Ling Lin
Chia Sui Lin
Chia Yi Lin
Chia Yin Lin
Chia Yu Lin
Chia Yun Lin
Chiao Hsin Lin
Chiao Hsuan Lin
Chiao Yen Lin
Chieh Ru Lin
Chien Ju Lin
Chien Mei Lin
Chien Ya Lin
Chien Yi Lin
Chien Yu Lin
Chih Hung Lin
Chih Shinn Lin
Chih Ying Lin
Chin Hui Lin
Chin Mei Lin
Chin Wang Lin
Chin Yao Lin
Ching Hui Lin
Ching Hung Lin
Ching Jung Lin
Ching Tzu Lin
Ching Yi Lin
Ching Yu Lin
Ching Yun Lin
Ching-Sheng Lin
Ching-Ying Lin
Chiu Jung Lin
Chiu Ling Lin
Chiu Ta Lin
Chiu Ya Lin
Chiu Yin Lin
Chu Yun Lin
Chuan Hui Lin
Chuen Ing Lin
Chun Chu Lin
Chun Hsien Lin
Chun Hsiung Lin
Chun Ju Lin
Chun Ting Lin
Chun Tse Lin
Chung Cheng Lin
Chung Chien Lin
Chung Hung Lin
Chun-Ting Lin
Cong Min Lin
Ding Han Lin
Fan Tsen Lin
Fang Se Lin
Fay-Teng Lin
Fei You Lin
Feng Yao Lin
Guan Sian Lin
Han Chun Lin
Han Wei Lin
Heig Chi Lin
Heng Hsin Lin
Ho-Hsin Lin
Hong En Lin
Hsiang Pin Lin
Hsiang-Yi Lin

Hsiao Chi Lin
Hsiao Chien Lin
Hsiao Chun Lin
Hsiao Hsuan Lin
Hsiao Lun Lin
Hsiao Ne Lin
Hsiao-Mei Lin
Hsin Hung Lin
Hsin Yi Lin
Hsing Chen Lin
Hsing Hua Lin
Hsing Yu Lin
Hsin-Hong Lin
Hsiu Chih Lin
Hsiu Ling Lin
Hsuan Chih Lin
Huei Wen Lin
Hui Ching Lin
Hui Mei Lin
Hui Ping Lin
Hui-Ming Lin
Hung Wei Lin
Hung Yang Lin
Huo Yen Lin
I Ting Lin
Jen Chin Lin
Jengjong Lin
Jia Ying Lin
Jie-Yu Lin
Jing Shiang Lin
Ju Feng Lin
Ju Hui Lin
Ju Ting Lin
Jui Kun Lin
Jui Yun Lin
Jun You Lin
Kai Wei Lin
Kang Lieh Lin
Keng Feng Lin
Ku Feng Lin
Kuan Ting Lin
Kun Chiou Lin
Lee Chu Lin
Li Chin Lin
Li Mei Lin
Li Ping Lin
Li Wei Lin
Ling-Hua Lin
Lin-Ru Lin
Man-Lee Lin
Mei Chih Lin
Mei Feng Lin
Mei Hui Lin
Mei Man Lin
Mei O Lin
Mei-Chin Lin
Mei-Lun Lin
Meng Shien Lin
Menhui Lin
Min-Chieh Lin
Ming Chen Lin
Ming Hui Lin
Ming Hung Lin
Ming Tang Lin
Ming Yi Lin
Mong-Chun Lin
Pei Hua Lin
Pei Yu Lin
Ping Yang Lin
Po Chang Lin
Po Chen Lin

Ruey Rong Lin
Shan Ju Lin
Shao-Ling Emily Lin
Sheng Yi Lin
Shih Chih Lin
Shih Chun Lin
Shih Tsung Lin
Shing Ru Lin
Shiow Ching Lin
Shu Chen Lin
Shu Chuan Lin
Shu Fang Lin
Shu Fen Lin
Shu Hui Lin
Shu Hung Lin
Shu Ju Lin
Shu Wan Lin
Shu Yu Lin
Shu-Hui Lin
Shu-Hwa Lin
Shun Yu Lin
Siou Ji Lin
Su Jung Lin
Su Mei Lin
Sung Chih Lin
Szu Chi Lin
Ta-Wei Lin
Te Hwa Lin
Tien Ling Lin
Ting Li Lin
Ting Sheng Lin
Tsang Chi Lin
Tsu-Hsin Lin
Tsung Wei Lin
Tzu Chou Lin
Tzu Yen Lin
Wan Ju Lin
Wan Jung Lin
Wang Sheng Lin
Wei Lin
Wei Chien Lin
Wei Chih Lin
Wei-Hsun Ryan Lin
Wen Kwu Lin
Wen Lung Lin
Wen Pin Lin
Wen Tzu Lin
Wen Yao Lin
Wu Hsiung Lin
Ya Huei Lin
Ya Hui Lin
Ya Lan Lin
Ya Ling Lin
Ya Ping Lin
Ya Shu Lin
Yahui Lin
Yang Chieh Lin
Ya-Wen Lin
Ya-Ying Lin
Yen Chih Lin
Yen Yu Lin
Yen Yu Lin
Yi Chun Lin
Yi Hsien Lin
Yi Hsuan Lin
Yi Ting Lin
Yi-Chien Lin
Yi-Ling Lin
Yin Lin
Ying Jen Lin
Ying Ju Lin

Yu Bao Lin
Yu Cheng Lin
Yu Chieh Lin
Yu Ching Lin
Yu Chu Lin
Yu Fan Lin
Yu Huei Lin
Yu Lin Lin
Yu Ping Lin
Yu Rong Lin
Yu Shen Lin
Yu Sheng Lin
Yu Ting Lin
Yu Yu Lin
Yu Yuan Lin
Yuan Hung Lin
Yueh Fong Lin
Yuh Jiuan Lin
Yu-Han Lin
Yuh-Feng Lin
Yu-Hung Lin
Yu-Jung Lin
Yu-Lung Lin
Yun-Chung Lin
Zi-Ping Lin
Ding Yuh Liou
Yi Ting Liou
Yu Nung Liou
An Jen Liu
Bo Cheng Liu
Cha Hua Liu
Chang Wei Liu
Chao Hsin Liu
Chao Lun Liu
Chen Tai Liu
Cheng Chi Liu
Chia Yu Liu
Chia Yung Liu
Chien Chia Liu
Chien He Liu
Chih-Kuang Liu
Chin Ju Liu
Chin-Lung Liu
Fang-Yu Liu
Guan Min Liu
Hao-Chung Liu
Hsiao Ling Liu
Hsiao Ying Liu
Hsin Chun Liu
Hsing Chen Liu
Hsin-Ju Liu
Hsiu-Chuan Liu
Hung Hsin Liu
I Jou Liu
Jen-Hsien Liu
Jenn Yeu Liu
Jia Ling Liu
Jui Pi Liu
Ken-Hung Liu
Kuan Hui Liu
Kuan Hung Liu
Kuei Hsiu Liu
Li Mei Liu
Lin Fang Liu
Lung Ying Liu
Man Ching Liu
Mei Chun Liu
Mei Ling Liu
Mei-Ling Liu
Min Yu Liu
Ming Chuan Liu

Pei Liu
Pei Yu Liu
Pi Hua Liu
Ru Ping Liu
Shu Min Liu
Shu Nu Liu
Shu Ying Liu
Shu Yu Liu
Shun-Ying Liu
Su-Chung Liu
Ting Kun Liu
Tsai Yun Liu
Tsu Chen Liu
Tsung Hsien Liu
Tsung Long Liu
Tung Shi Liu
Wan Chia Liu
Wen Hui Liu
Wen Yang Liu
Xin-Ning Liu
Xiu Han Liu
Ya-Fang Liu
Yang-Hsin Liu
Yaowen Liu
Yaping Liu
Yi Chen Liu
Yi Chi Liu
Yi Chun Liu
Yi Hsin Liu
Yi Shiuan Liu
Yi Ting Liu
Yi Ying Liu
Yi Yuan Liu
Yi-Ling Liu
Ying Hui Liu
Ying Lan Liu
Yuan Kai Liu
Yueh Chin Liu
Yueh Ching Liu
Yung Chang Liu
Yung Tsan Liu
Yung Yuan Liu
Chi Chin Lo
Fung Mei Lo
Hsiao Yun Lo
Hsin Tai Lo
Hsiu Ting Lo
Hui Wen Lo
Li Ching Lo
Mei Ching Lo
Pai Chen Lo
Rui Zong Camel Lo
Shou Min Lo
Shu Ping Lo
Wan Fang Lo
Wei Shuo Lo
Wei-Feng Lo
Yi Ching Lo
Yi Hung Lo
Yu Chen Lo
Yu Chin Lo
Yu Ming Lo
Yu Pei Lo
Yung Wen Lo
Ching Yu Lu
Hansheng Lu
Hsiao Chen Lu
Hsiao Chien Lu
Hsiao Ping Lu
Hsiao Ying Lu
Huei Ting Lu

Hung Cheng Lu
Jun Ting Lu
Junghua Lu
Kuan Chou Lu
Kung Ching Lu
Mei Chin Lu
Mei Lien Lu
Mei Pei Lu
Ming Hsiang Lu
Pei Chun Lu
Pei Tzu Lu
Shiou Rung Lu
Ssu-Ying Lu
Ting Ni Lu
Ting Yi Lu
Tingting Lu
Tsai-Lien Lu
Tuan Tuan Lu
Wen Liang Lu
Yeou An Lu
Yi Chen Lu
Yi Chun Lu
Yi Hua Lu
Yu Chen Lu
Yu Ling Lu
Yuankan Lu
YuTing Lu
Su Liang Luo
Wei Shiun Luo
Chiu Mei Ma
Chun Yen Ma
Hsiao Chin Ma
Juo Ying Ma
Chun Wei Mai
Li Lai Man
Li Chi Mao
Ya-Chen Mei
Chen Mei Ching
Hao Yu Ni
Tsuyung Ni
Hsing Hua Nien
Jen Chieh Niu
Lin Kuei Ou
Ming Chieh Ou
Ya Chi Ou
Zai Tian Ou
Chia Hui Pai
Jenn Yih Pai
Kuei Ju Pai
Yi-Chung Pai
Chi Chih Pan
Chiao Wen Pan
Chih Cheng Pan
Ho Sung Pan
Hsuan Jung Pan
Kuan Ju Pan
Li-Chin Pan
Mei Ling Melissa Pan
Meng Yin Pan
Wu Jen Pan
Yi-Ling Pan
Ying Yen Pan
Yu Tien Pan
Cho Pei Ying
Chi Hsun Pen
Hsiu Li Peng
Hung Kai Peng
Jui Fen Peng
Li Wen Peng
Mei Yu Peng
Mei Yun Peng

Sheng-Hsin Peng
Shih Wei Peng
Shu Yi Peng
Ting Huei Peng
Tzu Yun Peng
Ya Hui Peng
Ya-Chi Peng
Yi-Chen Peng
Yu Chieh Peng
Yu Jhu Peng
Hsiu Chuan Pin
Sze Wan Poon
Hsiang Chin Pu
Yi Ling Ren
Wu Jen Rong
Yang Su Rong
Siao Lan Ruan
Pe I Shan
Hsiu-Kan Shang
Chang Yu Shao
Ping Shao
Yu Fang Shao
Bey In Shen
Chang Ying Shen
Hua Lu Shen
Huan Yu Shen
I-Ting Shen
Iying Shen
Jung Kuang Shen
Li En Shen
Meng-Jin Shen
Shu Yin Shen
Shu Yu Shen
Ting Ying Shen
Ya Ping Shen
Yen Lun Shen
Yi-Ju Shen
Ying-Liang Shen
Yu Sheng Shen
Yung Chi Shen
Yungchung Shen
Xiao Gui Shi
Tiffany Shia
Jia Yung Shiau
Chien Yi Shih
Chien Yu Shih
Chih Chieh Shih
Hsin Fang Shih
Hui-Tzu Shih
Ming Hwa Shih
Pao Ling Shih
Pei Jung Shih
Pei Wen Shih
Shu Chuan Shih
Wen Hua Shih
Ya Ju Shih
Yen Rong Shih
Ying Te Shih
Yu Hung Shih
Yu Tsung Shih
Yu-Hwa Shih
Chien Hui Shin
Cheng Hsiung Shu
Hui Chuan Shu
Ming-Hui Shu
Yang Shu Fen
Yi-Ru Shyu
Ya Chi Sie
Chen-Yi Su
Chia Chueh Su
Chia Han Su

Chiao Ying Su
Chiu Hao Su
Feng-Zhao Su
Hao Hsiang Su
Hsiao Ling Su
Hui Tzu Su
I Wen Su
Jin-Chu Su
Jing Wen Su
Jo-Yun Su
Li Chun Su
Li Wen Su
Lindsay Su
Mei Chen Su
Min Hui Su
Pei Yun Su
Pin Chun Su
Shiou Chang Su
Shu Wan Su
Su Chen Su
Ting Yu Su
Tsung Ta Su
Tzu Ting Su
Wan-Ju Su
Yea Fang Su
Yeh Hsiung Su
Yi Hong Su
Ying Hua Su
Ying Ping Su
Yu Kai Su
Lee Yen Sue
Ka-Li Suen
Chien Li Sun
Chih Hsiung Sun
Hsu Chang Sun
Tzu-Ming Sun
Yu Shan Sun
Yu Ting Sun
Yu Yin Sun
Chao Ta Sung
Chin Feng Sung
Hsin Yu Sung
I Shiuan Sung
Karen Sung
Kuo Wei Sung
Min Tai Sung
Pei Chen Sung
Shiau-wen Sung
Su Fang Sung
Tsai Feng Sung
Ya Chien Sung
Yi-Ting Sung
Hung Hsuan Sherry Syh
Meng Syuan Syu
Chia Min Tai
Hui Fang Tai
Li Li Tai
Peng Cheng Tai
Yu Ping Tai
Yu Wen Tai
Yu Yen Tai
Yun Shan Tai
Chih-Tzu Tan
Guo Jyh Tang
Li Lin Tang
Shao Ping Tang
Shihyuan Tang
Kuo Te Cheng
Chih-Chung Teng
Chung Yi Teng
Li Wen Teng

Pei Chun Teng
Shih Lan Teng
Su Feng Teng
Su-Hsing Teng
Sui Yao Teng
Chenhsu Tien
Chia Chi Tien
Chieh Wen Ting
Shiu Hui Tong
Chang Pin Tsai
Chen Yu Tsai
Cheng En Tsai
Cheng Ying Tsai
Cheng-Jung Tsai
Chia Hui Tsai
Chia I Tsai
Chia Yuan Tsai
Chieh Shih Tsai
Chien-Chung Tsai
Ching Min Tsai
Ching Shiang Tsai
Ching-Ju Tsai
Chiou Uen Tsai
Chiufa Tsai
Chiung Chao Tsai
Chi-Ying Tsai
Chun Chi Tsai
Chun Chieh Tsai
Chung Chi Tsai
Chung Heng Tsai
Der-Sheng Tsai
Hsin-Yi Tsai
Hsiu Ching Tsai
Hsiu Feng Tsai
Hsueh Min Tsai
Jih Yih Tsai
Jing Huey Tsai
Joann Tzu-Chen Tsai
Jui Fang Tsai
Jung Chi Tsai
Kai Ting Tsai
Kevin Tsai
Kui Fen Tsai
Kun Lin Tsai
Lae Yi Tsai
Ling Yu Tsai
Mang Ping Tsai
Mei Chen Tsai
Mei Fang Tsai
Meng Hsia Tsai
Meng Ju Tsai
Meng Tzu Tsai
Min Wei Tsai
Min Yeh Tsai
Ming Cheng Tsai
Ming Juan Tsai
Ming Ko Tsai
Minhua Tsai
Nien Ting Tsai
Pei Chun Tsai
Pei Hsiu Tsai
Pei Ting Tsai
Pei Yi Tsai
Pei Ying Tsai
Pi Ju Tsai
Po Ching Tsai
Po Tien Tsai
Shang Chih Tsai
Sheng Han Tsai
Sheng-Chang Tsai
Sheng-Hung Tsai

Shou Hsun Tsai
Shu Ling Tsai
Shu Min Tsai
Shu-Fen Bena Tsai
Siang Chun Tsai
Su Mei Tsai
Sung Yu Tsai
Tsai Mai Tsai
Tsai Yin Tsai
Tsui Fen Tsai
Tsung Han Tsai
Tsung Yao Tsai
Wan Lin Tsai
Wei Chun Tsai
Wen Ling Tsai
Ya Chien Tsai
Ya Chu Tsai
Ya Ting Tsai
Ya-Ju Tsai
Yen Ju Tsai
Yi Chen Tsai
Yi Chun Tsai
Yi Ting Tsai
Yi-Ling Tsai
Yu Cheng Tsai
Yu Ling Tsai
Yuchieh Tsai
Yu-Fen Tsai
Yu-Hsin Tsai
Yun Lin Tsai
Yung Chi Tsai
Wen-Hsin T'Sai
Melody Tsan
Lih Chung Tsao
Meei Mei Tsao
Mei Hui Tsao
Sheng Fa Tsao
Terrisa Tsao
Tien Chieh Tsao
Wei-Chieh Tsao
Yung Chi Tsao
Yu Jiin Tsay
Ying-Hui Tsen
Chao En Tseng
Chi Lin Tseng
Chiang Tseng
Ching Ju Tseng
Chiung Wei Tseng
Chi-Wen Tseng
Chun Chun Tseng
Chun Yu Tseng
Hsin Yi Tseng
Hui Shan Tseng
Hung Tseng
Li Chin Tseng
Li Chun Tseng
Li Ping Tseng
Miao Ju Tseng
Pei Hua Tseng
Pi Chu Tseng
Pi Ling Tseng
Shih Wei Tseng
Su Er Tseng
Su Wen Tseng
Suchen Tseng
Ting Chieh Tseng
Vita Tseng
Wan Ju Tseng
Wan Zong Tseng
Wei-Chieh Tseng
Ya-Li Tseng

Yi Tun Tseng
Ying-Ya Tseng
Yu An Tseng
Yu Ling Tseng
Yuan Hao Tseng
Chun Chi Tsou
Jen-Chuan Tsou
Pei Jung Tsou
Shu Fen Tsou
Shu Yen Tsou
Wanju Tsui
Chien Yeh Tu
Chi-Huang Tu
Hsin-Yu Tu
Mei Hui Tu
Meng-Tien Tu
Pinghsun Tu
Sheng-Hsiao Tu
Shu Chin Tu
Shu Hua Tu
Shu Yuan Tu
Tzu Lin Tu
Yi Hua Tu
Yufan Tu
Hsueh Kang Tung
Li Hua Tung
Li-Ting Tung
Pei Ling Tung
Rachel Tung
Shu Chi Tung
Shu Ching Tung
Tsung Han Tung
Chi Jang Tzeng
Huei-Jiun Tzeng
Yi-Chuen Tzeng
Yi An Wan
An Chun Wang
Chao Hsing Wang
Chao Yu Wang
Chi Kang Wang
Chia Chung Wang
Chia En Wang
Chia Lun Wang
Chia-Ping Wang
Chien Cheng Wang
Chien Chun Wang
Chien Hsun Wang
Chien Mao Wang
Chi-Hsiang Wang
Chin Chuan Wang
Ching Jenn Wang
Ching Mei Wang
Ching Ting Wang
Ching Wen Wang
Chiung-Yi Wang
Chong Shyan Wang
Chun Hua Wang
Chun Hui Wang
Chun Pi Wang
Chun-Ping Wang
Cindy Wang
Diing Bih Wang
Fa I Wang
Feng Yu Wang
How Ren Wang
Hsiang Fu Wang
Hsiao Ting Wang
Hsiao Yun Wang
Hsiu Lan Wang
Hsuan-Yin Wang
Hui Chuan Wang

Hui Lien Wang
Hui Yao Wang
HuiChi Wang
Huiman Wang
Hung Hsiang Wang
Hung-Chun Wang
I Wen Wang
Jhen Yu Wang
Jheng Ya Wang
Jui Yi Wang
Jui-Yu Wang
Kuo Tai Wang
Lan Yi Wang
Li Hua Wang
Li Hung Wang
Li Ling Wang
Liang-Huei Wang
Li-Jen Wang
Mei Ling Wang
Mei Shu Wang
Mei-Ying Wang
Min Hsien Wang
Mu Chuang Wang
Pei Jan Wang
Pei Jen Wang
Pi Lan Wang
Ren Jing Wang
Ruo Bai Wang
Shih Ning Wang
Shih Rong Wang
Shu Rong Wang
Shwu-Ling Wang
Siang Hua Wang
Su Yun Wang
Szu-Hui Wang
Tien Mei Wang
Ting Tzu Wang
Tzer Tzu Wang
Tzu Hao Wang
Tzu Hau Wang
Tzu Hsin Wang
Tzu Ping Wang
Tzu Yi Wang
Tzu-Yin Ann Wang
Vicky Wang
Wan Jou Wang
Wei Pin Wang
Wei Ping Wang
Wen-Yann Wang
Ya Ju Wang
Ya Ling Wang
Yan Huei Wang
Yen Chun Wang
Yen-Ling Wang
Yi Zhi Wang
Yin Kuei Wang
Ying Hsin Wang
Ying Luen Wang
Ying Ting Wang
Yu Chi Wang
Yu Chieh Wang
Yu Hsiang Wang
Yu Hwa Wang
Yu Tzu Wang
Yuan Ting Wang
Yun Chi Wang
Yun Wen Wang
Yun-Chiao Wang
Yung Chieh Wang
Yu-Ting Wang
Chia Ling Wei

Chun Ta Wei
Hsiu Mei Wei
Jung Chieh Wei
Ju-Yu Wei
Kuang Liang Wei
Kuo Hua Wei
Shih Chiao Wei
Shih Hsun Wei
Shihshan Wei
Tzu-Ching Wei
Ya Mei Wei
Ying Huang Wei
Chia Ling Wen
Ching Yao Wen
Hung Chih Wen
Kai Ting Wen
Shu Ying Wen
Yao-Chih Wen
Yu-Hao Wen
Hui Min Weng
Li-Ping Weng
Mei Hua Weng
Shufen Weng
Wei Ting Weng
Wei-Siou Weng
Yi Ting Weng
Chen Chuan Wong
Rui Chin Wong
Tuan Tuan Wong
Ai-Fen Wu
Bi Lin Wu
Bo-Han Wu
Chao Hsien Wu
Chao Ling Sophia Wu
Chen-Feng Wu
Cheng Hao Wu
Chi Ying Wu
Chia Chen Wu
Chia Hui Wu
Chia Jung Wu
Chia Ta Wu
Chia-Ling Wu
Chiao Ching Wu
Chien Ping Wu
Chih Hsien Wu
Chin Lien Wu
Ching Ching Wu
Ching Ju Wu
Ching Yang Wu
Ching Yi Wu
Chiu Mei Wu
Chiung-Chuan Wu
Chuan Li Wu
Chun Ju Wu
Chun Te Wu
Dai Yu Wu
Day Sun Wu
Fanyou Wu
Fui Wu
Hsiao Chen Wu
Hsiao Mei Wu
Hsin Yu Wu
Hsin-Jung Wu
Hsiu Chen Wu
Hsiu Chu Wu
Hsiu Fang Wu
Hsueh Chiao Wu
Hsueh-Man Wu
Huei Yuan Wu
Huey-Ling Wu
Hui Chuan Wu

I Ping Wu
I-Chiien Wu
Jin Min Wu
Jong Yeong Wu
Jung Ju Wu
Jyong Sian Wu
Kane Wu
Kuan Wei Wu
Kuen-Shan Wu
Kuo Hsing Wu
Kuo Ting Wu
Li Hsueh Wu
Liping Wu
Mei Chan Wu
Mei Fang Wu
Mei Fen Wu
Mei Huan Chloe Wu
Mei Yen Wu
Mei-Hsiu Wu
Mei-Rong Wu
Meng Hsu Wu
Meng-Chieh Wu
Miin Lang Wu
Min Hua Wu
Ming Che Wu
Ming-Hsien Wu
Pei Chen Wu
Pei Hua Wu
Pihua Wu
Ping Chin Wu
Po Han Wu
Shao-Ping Wu
Sheng Hua Wu
Shiau Wen Wu
Shin Ting Wu
Shu Chun Wu
Shu Yi Wu
Shu-Fen Wu
Shun Mei Wu
Su Hsing Wu
Szu Hui Wu
Sz-You Wu
Ta-Jung Wu
Ting Yu Wu
Ting Yun Wu
Tsai Shan Wu
Tung Huang Wu
Tung Lung Wu
Wan Chi Wu
Wei Hsun Wu
Wei Tu Wu
Wen Chang Wu
Ya Ju Wu
Ya-Mei Wu
Yan Yi Wu
Yaoguang Wu
Yi Chen Wu
Yi Chien Wu
Yi Kai Wu
Yi Lung Wu
Yi Syuan Wu
Yiling Wu
Yin Chen Wu
Yinhui Wu
Yu Che Wu
Yu Chuan Wu
Yu Jing Wu
Yu Ting Wu
Yu Tzu Wu
Yueh-Er Wu
Yuhan Wu

Yuh-Tyng Wu
Yung Nan Wu
Yu-Ting Wu
Ming-Xun Xie
Ho Ya-Han
Miao Hua Yan
Ceng Ju Yang
Chao Lung Yang
Chen Chen Yang
Chen Wei Yang
Chen-Hsun Yang
Chiao Jung Yang
Chien Chin Yang
Chih Wen Yang
Ching Hai Yang
Ching Hsuan Yang
Ching Rong Yang
Chin-Yin Yang
Chun Fang Yang
Chun Fen Yang
Chun Hang Yang
Chung Wen Yang
David Yang
Fang Ni Yang
Fu Mei Yang
Han Lin Yang
Hau-Wei Yang
Heng Min Yang
Hsi Ming Yang
Hsiu-Hua Yang
Hui Ching Yang
Hui Fang Winnie Yang
Huiling Yang
Hung Chang Yang
I Kuo Yang
Jen Jung Yang
Jin Yang
Kai Shu Yang
Kuo Shien Yang
Li Ji Yang
Lili Yang
Li-Mei Yang
Li-Yu Yang
Mei Yang
Mei Hui Yang
Mei Ling Yang
Meng Shan Yang
Ming Che Yang
Ming Hsueh Yang
Ming Hui Yang
Ming Ming Yang
Ming-Fang Yang
Pei Wen Yang
Peichi Yang
Shen Chieh Yang
Shih Yuan Yang
Shirley Chung-Pang Yang
Shu Chun Yang
Shu Fang Yang
Shu Ho Yang
Shu Wen Yang
Shu-Hua Yang
Shun Min Yang
Shu-Rong Yang
Su Hui Yang
Su Yi Yang
Sue Fang Yang
Sy Tyng Yang
Tsan Yu Yang
Tzuyuan Yang
Wang Jung Yang

Wen Feng Yang
Wen Hsin Yang
Woanping Yang
Ya Hui Yang
Ya Ru Yang
Yao Sheng Yang
Yi Hsuan Yang
Yi-Ching Yang
Yin Ju Yang
Yu Hsuan Yang
Yu-Chi Yang
Chin Jen Yao
Hsiao Yun Yao
Pei Yu Yao
Ya Ling Yao
Ying Jyun Yao
Ming Hong Yau
Chen Hsuan Yeh
Chia Lun Yeh
Chih Yuan Yeh
Chuang Te Yeh
Der Tser Yeh
Fang-Ling Yeh
Hsin Ying Yeh
Jo-Mei Yeh
Jung Chun Yeh
Lan Hsiang Yeh
Ming Feng Yeh
Nai Chi Yeh
Pei Hsin Yeh
Pin Ling Yeh
Shu Ling Yeh
Shu-Chen Yeh
Te-Hua Yeh
Ting Chia Yeh
Ya Ting Yeh
Yi Chen Yeh
Yu Shan Yeh
Yu Tang Yeh
Yu Yi Yeh
Yung Cheng Yeh
Jung Yu Yen
Chang Yang Yen
Fei-Shen Yen
Hsin Ju Yen
Hsiu Chun Yen
Hsiu Ting Yen
Huang Yu Yen
Hui-Chen Yen
Li-Yu Yen
Tsai Yi Yen
Ya Chun Yen
Pei Ju Yi
Pi Yun Yi
Tzu Ling Yi
Chiang Yi Ching
Lin Yi Shun
Chia-Hui Ying
Wen-Ting Yiu
Chao Chin Yu
Chao Yang Yu
Cheng Chih Yu
Chia Chieh Yu
Chia Chun Yu
Chia-Ling Yu
Chien-Lin Yu
Chih Yung Yu
Chin Lung Yu
Chin-Hua Yu
Chiunghua Yu
Der Shiann Yu

Elaine Yu
Hsiao Yun Yu
Hsin Ju Yu
Hui Wen Yu
Janmin Yu
Jung Che Yu
Li Chun Yu
Lii Hoang Yu
Mei Hsiang Yu
Ming-Chu Pearl Yu
Min-Ping Yu
Pei Yeh Yu
Shen-Chou Yu
Shih Ting Yu
Shu Chun Yu
Shu Mei Yu
Shu Ying Yu
Suhua Yu
Taihsin Yu
Ya Han Yu
Ya Ling Yu
Yen Hsin Yu
Yi Ting Yu
Chen Yu An
Hua Kuo Yuan
Shao Wu Yuan
Shih-Hsiu Yuan
Shuo Wei Yuan
Yun Yi Yung
Ya-Ting Zeng
Chang Qing Zhang
Yu Xin Zhang
Ting Ting Zheng
Yi Jun Zhou

Thailand

Tulapawn Achananuparp
Thatchanok Chanyanuparp
Hung-Chun Chen
Chia-Huang Cheng
Cherng Jiun Shiah

Trinidad and Tobago

Laura Garcia
Dana Perry
Paulette Phillips

Turkey

Evren Devrim Celik
Derya Işözen
Umut Pasin
Shilei Ruan
Pelin Turkgungor

Uganda

Ivan Kagoro
Edward Kiwalabye
Norah Namataka

United Arab Emirates

Mohamed Ezzat Abdel Razek
Firuzi Eddy Adul Kotwal
Payal Agrawal
Hanafy Helmy Ahmed Abdallah
Sitara Akbar
Syed Shozeb Ali
Tania Amin Muhammad
Peter Aswad
Jasbir Bindra
Junaid Bukhari
Amrinder Singh Chawla
Wen-Yang Chien
Suzanne Chong
Shaza Mansoor El Sheikh
Mohamed Fairooz
Pooja Gajria
Nathalie Gandhi
Andrea Henriques
Vignesh Jayachandran
Sunil John
Rose Joseph
Syed Zain Khalid
Mohammed Mohsin Kilpadi
Jiju Mathew
Ajaymohan Mullackal
Rajesh Nair
George Nakhoul
Eunice Ong
Manal Osman Ibrahim
Abhinav Pahwa
Manoj Kumar Palangadan Illath
Rittika Palta
Chandra Ramachandran
Jayaraj Ramakrishnan
Nageswaran Raman
James Rickett
Ahmed M. Aly Saleh Shamroukh
Bruno Salomoni
Suresh Sambasivam
Cyril Samson
Vinod Sankaranarayanan
Shirish Shah
Vinay Kumar Shetty
Jagjit Singh
Mohammad Ayaz Soleja
Simi Sundaram
Vikas Thorat
Tanya Tourani
Srisudharsan Vasudevan
Sarah Wrigley
Alan Zachariah
Moamen Tharwat Zaki Ali
Kamal Zein

United Kingdom

Adejoke Adeniji
Md Ashraful Alam
Olajumoke Badejoko
Jack Bateman
Nicholas Bobb
Julia Bridcut
Malcolm Campbell
Phoebe Chen
Katarina Cook
Graham Cromie
Louise Cruickshanks
Alexander Denley
Nektarios Diamantis
Desiree Djete Epse Kouakou
Martin Dudas
John Durnian
Kasia Dyczkowska
Blake Empey
Indu Garg
Maria Glebova
Nathan Hamilton

Jon Harvey
Colin Hayes
Adnan Hussain
Vladimir Ivanov
Christina James
Jessica Jansen
Justin Johnson
Mohammed Junnayd
Farzana Kabani
Li Wen Kao
Dhipersaud Khemraj
Delia Kong
Jin Li
Abid Mahmood
Alison Marky
Joseph Martins
Richard McDowall
Khalid Meah
Denise Medea
Stephen Montgomery
Emma Moore
Laetitia Mottet
Gillian Newman
Anna Nowak-Jabrane
Clodagh O'Connor
Craig Osborne
Archana Ravindran
Shantay Scorgie
Adam Sparks
Richard Talbut
Gemma Theoff
Judith Thompson
Costel Adrian Timofte
Salvatore Vitiello
Louise Wallace
David Waterfield
Peter Wood

United States

Agustin Raymund Abad
Roaa Al-khair A. Younis
Randa Abdelhamid
Priti Abraham
Aykut Acar
Ryan Aceste
Laurie Adams
Helen Adelman
Olubunmi Adeola
Candace Adkins
Robert Adler
Tricia Adolph
Ann Aerts
Shraddha Agarwal
Nikhil Aggarwal
Ann Aguilera
Jamal Ahmad
Nuha M. Ahmed Mohamed
Sukhrob Akhmedov
Sadia Akhter
Sheila Alabrudzinski
Alejandro Alcala
Hamad Alhelal
Elena Allen
Cory Allender
Gavin Alleyne
Zachary Allshouse
Peter Alvarado
Luis Alvarez
Purvika Amin
Catherine Anderson
Laura Anderson
Michelle Anderson
Patricia Anderson
Zoya Annekova
Sandro Aranzabal-Giordano
Ana Maria Araujo
Mateo Arbelaez
Renan Arnalde
Shivani Arora
Marissa Arredondo
Damon Arrington
Paul Artley
Zoya Ashirov
Jenay Austin
Cheryl Aversa
Steve Baca
Stephanie Bacue
Joseph Badalamente
Chad Baer
Amer Baghajati
George Baican
Tarvinder Bains
Najeed Baker
Kagen Balco
Hiranmayee Baldev
Thomas Banasik
Michael Barredo
Tiffany Barrett
Guadalupe Barrios
Jennifer Barta
Barbara Bartley
Jane Barto
Jennifer Basedow
Jessica Basham
Pierre Basmaji
David Bass
Brad Bates
Matthew Beckwith
Thomas Bedkowski
Adrienne Bednarz
Rosmary Bedoya
David Behm
Biruk Bekele
Leesa Bell
Shavonn Bell
Dave Bellan
Roseann Bellus
Trimaine Belton
Justine Bemis
Cindy Bender
Snehal Bendhale
Melany Benning
Laura Benson
Ryan Berent
Tyler Berg
Guillermo Besserer-Ochoa
Lorraine Betancourt
Justin Beufve
Robert Beverly
Michael Bishop
Gregory Bissonnette
Caroline Bitar
Elizabeth Black
Heather Blair
Yvette Blake
Cynthia Bland
Shawn Blyth
Christopher Boersma
Gemma Bookless
Jacqueline Bosak
Brian Bostak
Bintia Boure
Jonathan Boyd
Ralph Brack
Jacob Brackens
Amy Bradt
Roger Branco
Stacy Brashear
Tennille Brathwaite
Georgee Brazil
Lindsay Brennan
Michelle Brewster
Jacob Brink
Steven Bronnenberg
Shannon Brooks
Rachel Brown
Alicia Browne
Stephen Bruce
Thomas Bruno
Charles Bruton
Vanessa Bryant
Christina Buhta
Edgar Bulawan
Alecia Burgard
Sara Bushen
Douglas Bushman
Jody Butzen
Davida Bynum
Rachel Byrd
Steven Byrd
Christa Cahill
John Calderon
Richard Calderone
Kelly Caltabiano
Alistair Cameron
Matthew Cameron
Margaret Capoccia
Marcos Caraballo
Julius Caranda
Ladislao Carballosa
John Cariker
Ryan Carita
Luz Carlos
Rebecca Carpenter
Renard Carpenter
Travis Carter
Shawn Carty
Erin Casey
Rosa Castillo
John Castles
Ervey Castoreno
Ximena Castro
John Castronovo
Craig Cathcart
Cheryl Caval
Sahng Seok Cha
Huanchee "Aaron" Chan
Ronny Long Chan
Kristine Chandler
Nischal Chandra Mohan
Geraldine Charles
Edward Charlton
Michael Chasen
Anil Chaturvedi
Susan Chen
Yi-Yu Chen
Yu Fan Chen
Zhipeng Chen
Jonathan Cheng
Ramkumar Cherukupalli
Danny Cheung
Sharon Chew
Yvonne Chiau
Chia Hui Carol Chien
Vipul Chokshi
Jaeyun Chong
Wen-Yen Chou
Brian Chu
Diego Chumaceiro
Hansol Chung
Stephanie Cipriano
Dustin Cladis
Jonathon Clair
Miranda Clark
Quinita Clark
Shirley Clark
Teresa Clemente
Bradley Clemmer
Mary Coleman
Robert Coleman
William Collins
Amy Collucci
Kenneth Connaughton
Devin Constantine
Kyle Contente
Gregory Contino
Mario Contreras
Christian Cooper
Kenzie Cornelius
Michael Cornelius
Diana Cortes
Eric Cothran
LaCresha Crawford
Robert Crawford
Karen Crespo
Matthew Cridge
Amber Criscone
John Crotty
Gary Cuddy
Shepard Cynamon
Ryan Dalrymple
Manan Dani
David Dann
Subrahmanyam Darbha
Ryan Darling
John DaSilva
Vanessa Daszewski
Steven Dato
Jezzica David
Tanya Davis
Ashley Elizabeth Day
Yolanda Dean
Yvonne Debesa
Jeffrey DeCicco
Charles Deckshot
Peggy Deel
Dia Dekantios
Kristin Delong
Bruno DeOliveira
Hardik Desai
Sarah Desrosiers
Antonela Destanisha-Martini
Adam Deutsch
Anny Devargas
Amrita Dhingra
Patrick Diamond
Patricia Diaz
Chris DiBuono
Matthew Digiacobbe
Courtenay Dillard
Jarom Dilworth
Iliyana Dimitrov
Russell DiNaro
Lesurma Dixon
Matthew Dixon
Christina Dizer
Marine Doguzashvili
Lisa Dooley
Thomas Dooley
Mark Doyle
Pamela D'Sa
Neil D'Souza
Bruce Dubinsky
Charlotte Dufour
Michelle Duga
Geris Duma
Kathy Dunn
Nick Duva
Kelly Dynes
Paul Eastwood
Rodney Echard
Marie Edouard
Barbara Edwards
Zachary Edwards
Shiva Eftekhari
Erin Egan
Jeffrey Eig
Emily Elbert
Jordan Elias
Igor Elkun
Marcus Elliott
Anson Ellis
Sara Ibrahim Elnour Ibrahim
J. Peter Engler
Chaitanya Eranki
Judith Erickson
David Ernst
Dennis Ervin
Walter Estrada
Tyler Evenson
Mehran Faalzadeh
Ingrid Fabara
Clarissa Fabros
Dami Fadipe
Alan Fagan
Zaineb Faizi
Frank Fajardo Castro
Ashley Falvey
Faith Farella
Ryan Farnsworth
Nadira Fauder
Edlira Fejza
John Ferguson
Dominique Fernandes
Francisco Fernandez
Alyson Ferro
Ronnie Figueroa
Kay Fillingham
Jeannine Fisher
Sarah Fishwick
Dennis Fitzgerald
John Fitzgerald
Kristina Flagg
Debora Fletcher
Rebecca Flynn
Christopher Foley
Daniel Foley
Anette Forde
Tanya Foster
Heather Frase
Andrew C. Fried
Anne Fuehrer
Robert Fuentevilla
Taeko Fukaishi

Jermaine Funchus
Anthony Fuschetto
Nuha Ali Gadkarim Ali
John Gadziala
Jaime Gaffud
Michelle Gainer
Denis Gallagher
Shane Galster
Shakthi Ganesan
Jose Garcia
Kevin Garcia
Maria Garcia
Megan Garcia
Dan Gardner
Manon Gavalda
Samuel Gen
Santhosh George
Edward Gerovian
David Gers
Ed Gertsberg
Adina Gherghian
Anna Gialaboukis
Dawn Giglio
Andrew Giles
Ethan Gill
Grant Gill
Laura Girten
Donna Glazer
Nancy Glynn
Mark Goldstein
Ivan Gomez
Altagracia Julissa Gonzalez
Blake Goodsell
Sandra Gould-Morais
Jon Graf
Linda Graff
Tamura Grant
Douglas Greenberg
Marc Greenberg
Antonio Greenidge
Jennifer Greenwell
Mary Gregorius
Byron Gregory
David Griesbach
Sharon Griffith
Timothy Griskey
Scott Grissom
Sabrina Grunewald
Eugenia Guajardo
Victor Guerra
Luis Guerrero
Deana Gum
Xiyi Guo
Amit Gupta
Veronique Guy
Susana Guzman
Joseph Haddock
Stephen Hagan
Robert Hale
Frederick Hamble
Ali Hamdan
Steven Hanzi
Keith Harding
Mallory Harrington
Andrew Harrower
Ariadna Hatcher
Julie Havrilla
Joshua Hawkins

Enrique Hayem
Michael Hazelwood
Agnes Hendarmin
Adina Henderson
Jami Henson
Linetty Herbert
Kim Herd
Vanessa Hernandez
Scott Hibbard
Michelle Highland
John Hill
William Hilton
Aubrey Hines
Erin Hitchens
Kayla Hohlt
Luis Holguin
Lauren Hollingsworth
Jared Holmes
Vernon Hoosier
Robert Hopkins
Hsiang Yao Hsu
Yan Huang
Yen-Hua Huang
Yu-Ching Huang
Megumi Huebert
Alexandra Hughes
Randle Hughes Jr.
Amy Hull
Marta Humienik
Collin Hunt
Ian Hunt
Georgia Hutton
Tracey Hwang
Shannon Inglesby
Yau Yin Eva Ip
Tomeka Isaac
Laura Itani
Paul Iya
Michele Jackson
Edward Jacobson
Joseph Jacobson
Marissa Janco
Deborah Janis
Robert Jefferson
Nicole JeNaye
Michael Joens
Paige Johnson
Robert Johnson
Paul Faulkner Jones
Michael Joseph
Ajay Joseph Baby
Andrew Josephy
J.R. Joyce
Maryia Kachan
Robert Kadel
Jarred Kahan
Radost Kandevadimitrov
Minwook Kang
Jasmine Kantor
Andrew Kaplan
Michael Kaplan
Donna Kapotas
Julie Kappenman
Scott Karem
Ariana Karzai
Chad Kasler
Sekhar Babu Katkam

Gurleen Kaur
Colleen Kavanagh
Kristen Kavanaugh
Lauren Keefe
Catherine Keeran
Scott Keller
Daniel Kelly
Mary Kelly
Stacie Kelly
Sharon Kelly-Watson
Kristin Kennedy
Mary Ann Kennedy
Christopher Kent
Sokvouth Keo
Angela Kern
Tehsin Khokhar
Phouthong Khousakoun
Ayako Kigoshi
Jessica Kim
Lina Kim
Sunghi (Stella) Kim
Yong-Tae Kim
Abraham King
Megan King
Kelly Kisling
Koffi Klu
Garin Knott
Phillip Koeber
Katie Kogler
Amanda Krieg
Daniil Krivov
Erin Kruth
Chi Tat Ku
Denise Kussard
Oleksii Kuzmenko
Yanna Kvurt
Calvin Kwan
Jennifer L. Sanchez
Gianluca La Manno
Robert La Porte
Lori LaChapelle
Nicholas Lacolla
Andrew Laing
Ching (Keith) Lam
Holly Lam
Jean Land
Joann Lang
Melissa Lanning
Christopher Laughner
Michael Lauricella
Daniel Lautenschlager
Elaine Leadlove-Plant
Mauricio Leandro
Anthony Lear
Sharon Lebold
Kestutis Ledas
John Spencer Lee
Kenneth Lee
Marian Lee
Yoojin Lee
Nadezhda Leonova
Adrienne Lerro
Manuel Lewis
Ryan Lewis
Wuen Sin Li
Wan Xian Donna Liang
Wenguang Liang
Xingfen Liang

Katherine Liaw
Judy Lim
Hui-Ting Lin
Miao-Shan Lin
Yu-Chang (Stephen) Lin
Xibei Liu
Amanda LoCicero
Joshua Lockard
Kevin Loiselle
Juana Lopez
Gabriel Lopez Gonzalez
Eileen Loria
Tony Lucas
Steven Lucia
Yarazed Lugo
Maria Alexandra Lugo Paris
James Lund
Christopher Lunsford
Radika Lutchman
Kevin Lynn
Crystal MacHendrie
Anuradha Madan
Linda Madryk
Zachary Malamud
Dolores Maldonado
Gaurav Mandilwar
Rosy Mares
Christopher Maricic
Melanie Markay
John Marley
Cleofas Martens
Grace Martin
Keenan Martin
Marilyn Martin
Melody Martinez
Ashley Masanto
Linda Masessa
Christopher Mason
Marc Massey
Joe Massie
Roger Massih
Jennifer Matheny
Helene Mathews
David Mayo
Sean McBride
Nakisha McCants
Scott McClain
Riqui McCorkle
Katherine McCormick
Leticia Mccracken
Kimberly McEnaney
Barbara McIntosh
Olivia McLeod-Smith
Ryan McNaught
Gabriel Mejia
Anthony Meli
Jared Melnyk
Joe Meloni
David Meltzer
Silvia Membreno
Ashley Meral
Marc Merrifield
Robert Mesarick
Thomas Metker
Sabine Michel-Zamor
Mitch Michniowski
Alexander Migirov

Christopher Milano
Kajon Maurice Miller
Kathryn Miller
Kevin Miller
Lisa Miller
Stephanie Miller
Lauren Milstead
Jessica Mitchell
Ahmed M. K. A. Ahmed
Ranya S. Mohamed Nour Khairy
Vincenzo Mohrfeld
Brandon Molina
Mya Aniese Mollaire
Amelia Moncayo
Danielle Money
Aya Montano
Valerie Montet
Craig Montgomery
Gerald Montieth
Bruce Moor
Charles Alexandre Moor
Emily Moore
Oscar Moraga
Patrick Moran
Berkis Morel Sanchez
Joseph Moreto
Jolene Morin
Kendrick Morton
Michael Moserowitz
François Mougnaud
Ana Muniz Alvarez
Alaina Murphy
Christopher Musser
Matteo Musso
Christopher Nadzam
Sandra Narvaez
Jane Natoli
Jeffrey Nelson
Siat L Ng
Noiy Nguyen
Tai Nguyen
Jasidney (Jay) Nichols
Yijun Niu
Blaise Njie
Frank Nonnenmacher
Khadar Noor
Ethan Nourse
Shelly Nunes
Timothy O'Brien
Ilisa Oddo-Scaduto
Rachel O'Keefe
Annie Olaverri
Stefanie Oliveira
Ross Olivier
Timothy O'Neill
Raluca Oniu
Valeka Oparah
Francisco Ortega
Richard Osei
Ron Oslin
Thomas Ostrowski
Arleni Pacheco
Jeffrey Pagliaro
Meghan Palanza
Agustin Palazón Hernández
Thomas Palermo
Anthony Palma
Kirkpatrick Pan

Stephen Panattieri
Josh Pang
Jessica Panikoff
Naddav Paran
Daniel Parodi
Brandon Parrish
Onika Parsons
Rikesh Patel
Madeline Patterson-Baleno
Inge Patton
Vaishnavi Pattumudi
Maria Paulino
Sarah Pearson
Patricia A. Pelaez Kawashima
Lisa Perard
Luis Pereda
Desiree Pereira
Luz Perez
Zurii Perkins
Brenda Perrotti
Natalie Perry
Azriel Peskowitz
Gerrit Petersons
Amy Petric
Nina Petrovic
Owen Phillips
Pamela Phillips
Cathy Philpott
Nefertiti Phipps-Smith
Claire Pige
Madelyn Pinlac
Chelsea Pirela
Amit Pitale
Matthew Plumb
Christopher Plymouth
Lisa Polkowski
Stacey Polreis
Kevin Polster
Philip Pomella
Scott Ponder
Heidi Pope
Caleb Popow
Alexandra Potes
Philip Potter
Suchithra Prabhuraj
Nica Price
Peter Prichodko
Sharon Pridgen
Amy Priputin
Bridgette Prise
Philip Prudenti
Valerie Pupchenko
Christian Purcell
Sravani Pusapati
Dara Queck
Natalia Quiroga
Hilary R. Huber
Simonetta Rafalska
Salima Rajan
Vidya Ramachandran
Marta Ramirez
Edwin Ramos
Betsabe Ramos Acosta
Randall Ranatza
Andrew Randaccio
Rajiv Ranjan
Stephanie Rankin
Aishwarya Ravuru Venkatesan
Babulal Rawal
Suzanne Ray
Edith Reber
Travis Redmon
Robert Reed
Alec Regitsky
Matthew Reilley
Nghi Reilly
Ornan Reinoso
Xiaomei Ren
Richard Rengel
Maria Francisca Reyes
Jennifer Reykjalin
Lindsey Reynolds
Freddy Ricart
Sylvia Rich
Andrea Rivera
Paul Rivera
Jun Young Ro
Sarah Robillard
Francisca Rodriguez
Terrence Romano
Jonathan Rome
Vincent Rooney
Margie Rosa
Shantel Rosemond
Karen Rosenthal
Kathy Rossi-Allen
Sheri Rostocil
Luke Rotter
Polly Rowe
Robert Rowen
Kimberly Roy
Daniel Runyan
Aleia Russell
Matthew Russell
Jumana Kawmy Rustom
Victoria Ruth
David Ryan
Deirdre Ryan
Maryanne Ryan
Huda Sabri
Majideh Salamat
Luis Salcedo
Isabel Samper
Carlos Sanchez
Salvador Sanchez
LaTonya Sanders
Claudia Sandoval
Libert Sang
Daniel Sankey
Hector Santana
Lissette Santiago Del Rio
Cesar Santos
Jhilam Sanyal
Bevon Sarara
Carlos Saravia
Nancy Sarokhan
Richard Savage Jr.
Mary Scarpelli
Ronald Schmick
Jonathan Schnader
Richard Schubring
Andrew Schwimmer
Kruzshander Scott
Skeeter Scott
Anna Seaman
William Selenke
Shivraj Seodarsan
Cynthia Serbia
Farida Shafee-Niranjan
Anuj Shah
Anuja Shah
Farwa Shah
Henali Shah
Cara Shamansky
Ju Yi (Angela) Shan
Sara Shankavaram
Jarett Shapiro
Homira Sharif
Phillipa Sheen
Chunlan Shen
Marisol Lee Sheppard
Samantha Sill
Danny Silva
Aylin Silveira
Gregory Simmons
Gurdeep Singh
Alanna Slater
Colby Smith
David Smith
Ligia Smith
Lawrence Smith III
Robert Sohr
Kyle Sokol
Sonia Solana
Lisa Somers
Noory Song
Danielle Sordi
Juana Soto
Souleymane Sow
Sega Sowe
Kellie Spawton
Barry Spilberg
Bernadette Sponsler
Richard Sposato
Neil Squires
Katherine Stabile
Heather Steele
Shannon Steele
Frank Stern
Gary Stevenson
Angela Stewart
Jocelyn Stewart
Ryan Stocking
Eric Stoppels
Michael Stufsky
Sumanth Sudheer
Margarita Sukach
Salem Suleiman
Kevin Sullivan
Lorraine Sumulong
Subhayan Sur
Matthew Sutton
Lisa Swagerty
Arianna Sweis
Gida Swenson
Allen Sztukowski
William Szymanski
Weiling Tai
Miho Tamegai
Danielle Tanderup
Thai Tao
Eric Tapper
Lance Tastet
Josh Taub
Lana Taubina
Antonio Tazón Fernández
David Teague
Michelle Teeter
Joann Teng
Sandy Tepper
Daniela Termersch
Christina Thayer
Latasha Thelemaque
Caroline Thomas
David Thompson
Erin Thompson
Wayne Thompson
Temitayo Tijani
Rasika Tipnis
Vesela Todorova
Zhao-Hui Tong
Erika Torrey
Trenton Toy
Perry Traina
Alex Treuber
Heather Trimble
Chetan Tripathy
Crystal Trout
Amity Turner
David Ulrich
Isaac Ungo
Prasad Upadhye
Yeisy Urbaez
Allen Valevich
Angela Vanover
Siril Varghese
Beatriz Vasconcellos
Christopher Vastine
Jagannathan Vasudevan
Dana Velasquez
Alvaro Velez
John Venezia
Alyssa Vera
Balbina Veras
Caroline Versace
Kelley Vescovi
Arvin Vigil
Mary Grace Villagomez
Alvin Vincent
David Vincent
Nicholas Vitale
Julie Vito
Toan Vo
Kosha Vriseno
Nicholas Vrudny
Marlin Wallace
Chiao Hui Wang
Shenghui Wang
Shin-Yu Wang
Yuan Winnie Wang
Mark Wargo
Grant Warnock
Jennifer Watkins
Terry Watson
Joel Waxman
Micaela Wegener
Sarah Weise
Eva Weiss
Jacqueline K. Wells
Gwen Weninger
Sabine West
Samuel Whatley
Michael Wheeler
Thomas Wickesser
LaShana Wiggs
Thomas Wight
Benjamin Wilbur
Michael Wilkes
Alex Williams
Catherine Williams
Eliza Williams
Krista Willwert
Christopher Winer
Sean Winn
Howard Wong
Joseph Woodruff
James Wycoff
Diana Xu
Wenting (Melody) Xu
Lee Yamane
Shao-Yi Yang
Shuchen Yang
Hitomi Yano
Melody Yeh
Weihong Yin
Zhenshu Yin
Katrice Yokley
Jacadra Young
Leslie Young
Steven Young
Inna Yudolevich
Fuat Yurekli
Jackelyn Zacarias
Diana Zadroga
Elizabeth Zamora Bluff
Nader Zaringhalam
Nurzhan Zhambekov
Junduo Zhao
Yi (Kevin) Zhao
Lin Zheng
David Ziman

Uruguay

Mariana Bardanca Rodriguez

Vietnam

Honglei Hao
Hsin-Chia Huang
Thi Ngoc Ly Nguyen
Oanh Tran

Yemen

Abdulsalam Ahmed AL-Baddai

Zimbabwe

Elisheba Chimbwanda
Neeta Joshi
John Maunganidze
Fionah Moyo
Simbarashe Mukoyi
Kudakwashe Ncube
Obias Runesu