

ACAMS[®]TODAY

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



Happy Birthday

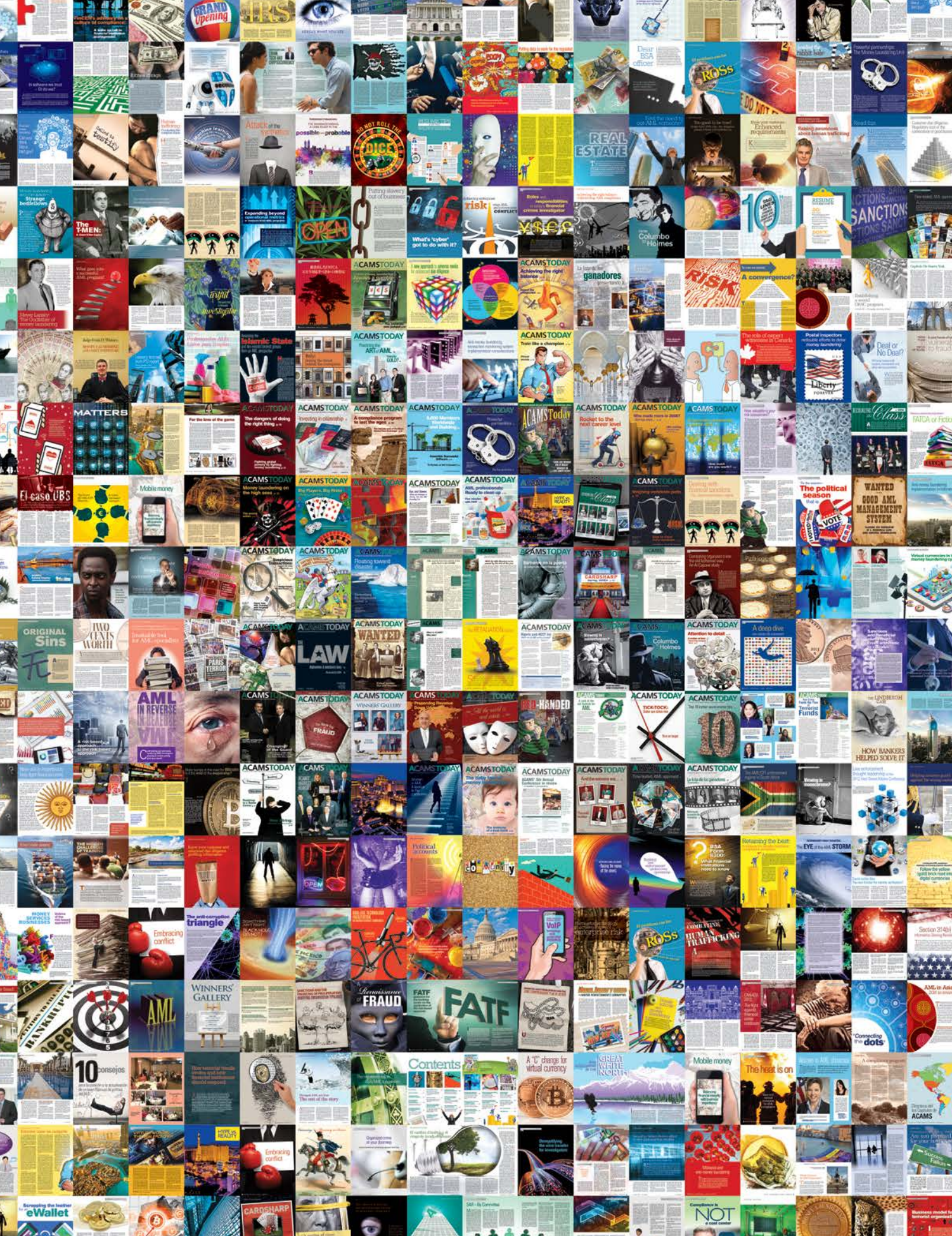
**TOP TALENT:
FINDERS KEEPERS**

MARCH–MAY 2017 VOL. 16 NO. 2

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

www.ACAMS.org
www.ACAMSToday.org





A man with short, dark hair and glasses, wearing a dark pinstriped suit jacket over a light blue collared shirt. He is looking off to the right side of the frame. The background is a bright, out-of-focus indoor setting.

Trace the
untraceable.

**Thomson Reuters CLEAR® delivers
trusted answers for anti-money laundering.**

Go deeper in your investigations and reveal connections other resources miss. With Thomson Reuters CLEAR you retrieve faster, more relevant results to help you find the answers. It's the easy way to uncover people, assets, businesses, affiliations, and locations. And with integrated reports you can easily share your findings.

Take your investigations further with CLEAR.
legalsolutions.com/clear

The intelligence, technology and human expertise
you need to find trusted answers.



the answer company™
THOMSON REUTERS®

Why spend 3 days with some of the brightest minds in AML audit or financial crimes investigations?

To earn the recognition you deserve for committing to protecting and elevating the status of your institution.



Earn the most exclusive and distinguished designation beyond CAMS that ACAMS offers. Email advancedcertification@acams.org to get started.

ACAMS
ADVANCED
CERTIFICATION
HANDBOOK & APPLICATIONS

CAMS
AUDIT

CAMS
FCI

acams.org

ACAMS

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.*



ACAMS® | Advancing Financial
Crime Professionals
Worldwide



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

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

| EDITORIAL AND DESIGN |

EDITORIAL ASSISTANT *Alexa Serrano, CAMS*

GRAPHIC DESIGN *Victoria Racine*

| EDITORIAL COMMITTEE |

CHAIR *Debbie Hitzeroth, CAMS-FCI*

Kevin Anderson, CAMS

Brian Arrington, CAMS

Edwin (Ed) Beemer, CAMS-FCI

Robert Goldfinger, CAMS

Jennifer Hanley-Giersch, CAMS

Eric Sohn, CAMS

Joe Soniat, CAMS-FCI

Amy Wotapka, CAMS

Elaine Yancey, CAMS

ACAMS Today © 2017 by the Association of Certified Anti-Money Laundering Specialists (ACAMS). All rights reserved.
Reproduction of any material from this issue, in whole or in part, without express written permission of ACAMS is strictly prohibited.

| SENIOR STAFF |PRESIDENT AND MANAGING DIRECTOR *Tim McClinton*HEAD OF ASIA *Hue Dang, CAMS-Audit*VICE PRESIDENT OF SALES *Geoffrey Fone, CAMS*GLOBAL DIRECTOR OF MARKETING *Kourtney McCarty, CAMS*HEAD OF EUROPE *Angela Salter***| SALES AND REGIONAL REPRESENTATIVES |**SENIOR VICE PRESIDENT OF BUSINESS DEVELOPMENT *Geoffrey Chunowitz, CAMS*REGIONAL HEAD *Sonia Leon, CAMS*HEAD OF AFRICA & THE MIDDLE EAST *Jose Victor Lewis, CAMS*DIRECTOR OF SPONSORSHIP & ADVERTISING DEVELOPMENT *Andrea Winter, CAMS***| ADVISORY BOARD |**CHAIRMAN *Rick A. Small, CAMS**Luciano J. Astorga, CAMS**Robert Curry, CAMS**William J. Fox**María de Lourdes Jiménez**Frank Lawrence, CAMS**Dennis M. Lormel, CAMS**William D. Langford, CAMS**Rick McDonell**Karim Rajwani, CAMS**Anna M. Rentschler, CAMS**Anthony Luis Rodriguez, CAMS, CPA**Nancy Saur, CAMS, FICA**Markus E. Schulz**Daniel Soto, CAMS***| ADVISORY BOARD SPECIAL ADVISORS |***Samar Baasiri, CAMS**Vasilios P. Chrisos, CAMS**David Clark, CAMS**Susan J. Galli, CAMS**Peter R. Hazlewood*

Contents



From the editor 8

Member spotlights 10

A message from the executive vice president. 12

The AML risk puzzle— What does AML risk really mean? 14
Understanding AML risk throughout the organization.

Are compliance testing functions aligned or overlapping? 20
The foundation to a sound compliance risk management structure.

Cyber security: Fake news, bots, botnets and click fraud 24
Challenges that fake news presents to financial crimes investigators.

De-risking and financial inclusion 30
The impact of de-risking and suggested solutions.

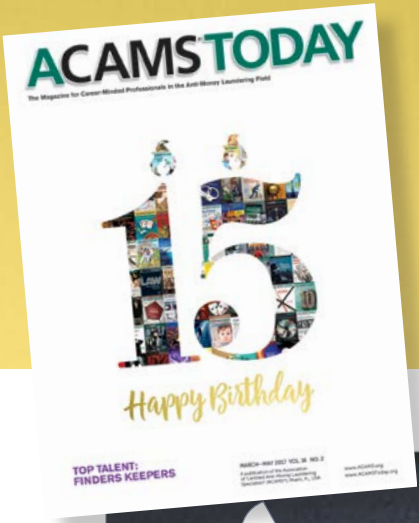
20 minute AML investigations 34
Getting the most out of your investigative resources.

Developing terrorist financing typologies for AML programs 38
Requirements needed to develop proactive counter-terrorist financing strategies.

John J. Byrne, CAMS: 15 years of ACAMS Today 45
A look back at the last 15 years of ACAMS Today and how the AML environment has since changed.

Dan Soto, CAMS: ACAMS' 15 years of growth 46
A discussion on the evolution of ACAMS and AML.

Karla Monterrosa-Yancey, CAMS: 10 years of an evolving ACAMS Today 48
Our editor-in-chief discusses her role in the production of the award-winning ACAMS Today magazine from start to finish.



ON THE COVER:

Celebrating 15 years of ACAMS Today 44
Happy birthday to ACAMS Today!

3,184
pages printed

50

ACAMS Today infographic and timeline.50
A glimpse of the last 15 years of the award-winning ACAMS Today.

An interlude with the ACAMS Today Editorial Committee.52
Our Editorial Committee shares their favorite part about being on the editorial team and their favorite articles.

A SARS and STRIPS retrospective.54
A look into the creation of ACAMS Today cartoons.

AML Classics58
A brief review of past ACAMS Today articles.



Hiding in plain sight62
The identification of ultimate beneficial owners and TBML in India.

How Fintech is changing the compliance landscape64
Finding the right balance in regulatory oversight for innovative financial products and/or Fintech startup partnerships.

Fintech: Two sides of the compliance coin.70
The benefits and challenges of Fintech.

Top talent: Finders keepers72
How to recruit, retain and build the perfect team.



Marketing 101: How an AML professional can increase marketability.78
The key to become and remain marketable.

Fourth time's the charm?82
A review of FATF's Fourth Round Mutual Evaluation Report for the U.S.' AML/CTF measures.

2017—Transition and transformation for Europe86
ACAMS' membership prepares for the 13th AML and Financial Crime Conference in London.

Meet the ACAMS staff87

CAMS and Advanced Certification graduates.88

Make a wish ACAMS Today

Welcome to *ACAMS Today's* 15-birthday celebration! In this edition of the magazine, we are celebrating all things *ACAMS Today*. In the last 15 years, the magazine has seen many changes, achieved milestones, seen a few firsts and even won a few awards. Of course, none of this would have been possible without the support, contributions and readership of our many ACAMS members, who I believe are the VIPs attending this grand celebration.

In the spirit of grand celebrations, it is time to unwrap the 15 gifts *ACAMS Today* has received:

1. A committed and knowledgeable Editorial Committee
2. A plethora of expert contributors
3. A dedicated ACAMS staff
4. A top-notch designer
5. A prestigious advisory board
6. Access to the latest AML and financial crime developments
7. Special editions dedicated to law enforcement, annual conferences and women in AML
8. A state-of-the-art website

9. The ability to be read in English, Spanish and Chinese
10. Specialized regional sections such as *Aspects of Asia*, *European Connect* and *The MENA Report*
11. A variety of member spotlights from around the world
12. Interviews with elite experts in the AML and financial crime prevention industries
13. Know Your Chapter contributions
14. Award recognitions from the publication sector
15. Premier magazine status for the financial crime detection and prevention professional

I hope you will enjoy this birthday edition of the magazine. We have dedicated a section of the magazine to *ACAMS Today's* 15-birthday celebration. The section contains interviews with John J. Byrne, CAMS, ACAMS executive vice president, Dan Soto, CAMS, ACAMS advisory board member and Ally Financial's chief compliance officer, and me. You will also find an interlude with the Editorial Committee and a retrospective of our entertaining SARS and STRIPS cartoon.



Finally, to top off the section, we have brought back some AML Classics for you to rediscover.

In addition to the celebration section, this edition has an assortment of articles ranging from career guidance such as our second headline article *Top talent: Finders keepers to Developing terrorist financing typologies for AML programs*. Other articles discuss the top challenges facing AML professionals like our two articles on Fintech and our cyber security article.

Finally, we hope all your wishes will come true and we hope you will help *ACAMS Today* with its birthday wish of remaining the premier magazine for the AML/financial crime prevention professional. **FA**

Karla Monterrosa-Yancey, CAMS editor-in-chief

SARSnSTRIPS™



Produced by: ComplianceComm



ATTIV/O

Break the case. Not the bank.

We deliver AML investigation savings up to 75%.

Optimize your AML case reviews, eliminate tedious evidence gathering and deploy consistently on a global scale. Not to mention, generate huge cost savings. That's the power of Attivio.

Visit attivio.com/ACAMS to learn more.



Rasheed A. Alanesi, CAMS, CPA, Sana'a, Yemen

Rasheed A. Alanesi is the assistant general and compliance manager at Yemen Kuwait Bank and the head of the Compliance Committee of Yemen Bank Association. He is a member of the National Committee for anti-money laundering and counter-terrorist financing (AML/CTF) and a member of the Risk Assessment team in Yemen.

Alanesi holds a bachelor's degree in accounting from Sana'a University. He is also a member of the Yemeni Association of Certified Public Accountants and he became a certified public accountant in 2002.

His career began as a bank inspector at the Central Bank of Yemen before moving to Crédit Agricole Bank—Yemen, where he held various positions (internal auditor, risk manager and inspection manager). In August 2005, he joined CAC Bank as the compliance manager until November 2009.

In addition, he was the executive manager as well as one of the founders of CAC Islamic Finance from 2009 to 2010 and he is the head of the Yemeni Organization, where he supports AML/CTF efforts.

**DID YOU KNOW THAT
184 MEMBERS HAVE
BEEN SPOTLIGHTED
IN THE ACAMS TODAY?**



John Moody, III, CAMS Brecksville, OH, USA

John Moody is a native of the greater Cleveland Ohio area and an accomplished CAMS professional. With a bachelor's degree in accounting from the University of Akron and a CRCM from the Institute of Certified Bankers, Moody's career covers a wide-banking background. He specializes in the analysis, creation and maintenance of anti-money laundering (AML) and counter-terrorist financing compliance programs that effectively integrate with financial institution business initiatives.

He started his career in 1981, working in various roles at seven different banks. These banks ranged from small U.S. banks to two large U.S. regional banks. Moody has been with KeyBank N.A. since April 2005 as the BSA officer and vice president. He is responsible for governing Bank Secrecy Act compliance topics and reports to the chief AML officer.

In addition, he is a founding director of the ACAMS Northern Ohio Chapter and was recently re-elected for another term. Moody participates in several AML peer call groups. In his current compliance manager role, Moody draws from various earlier roles, such as branch manager, accountant, compliance officer and senior compliance auditor. Moody's outside interests include traveling to the National Parks of the U.S. and Canada, hiking, rafting and canoeing in the Rocky Mountains and other locations as well as reading and watching science fiction.



Lynn Na Li, CAMS Shanghai, China

Lynn Na Li is an experienced anti-money laundering (AML) professional with over 13 years of related experience. In 2012, she received her Certified Anti-Money Laundering Specialist (CAMS) certification. She has worked in leading international banks, such as Mitsubishi, Sumitomo, BEA, and has headed AML departments. She also worked for Alibaba Group, the biggest Chinese online commerce company, leading legal, compliance, AML and the internal audit function. Currently, Li is the head of financial crime compliance at Standard Chartered Bank (China) Limited, leading a team of professionals in AML, sanctions, anti-bribery and corruption.

Li is also actively involved in the industrial events to promote better industrial practice and communication. She has been invited as a speaker at numerous ACAMS summits in China and has led her team to hold four AML Forums in Shanghai.

In 2006, Li represented China's banking industry by cooperating with FATF's initial mutual evaluation of China.

In 2008, Li led her team to help the People's Bank of China, the AML regulator in China, to establish the framework for the *Anti-Money Laundering International Practice and Reference* book and was responsible for the composition of the chapter "Japan AML practice." In addition, she was recently elected as the vice chairman of the AML working group of Shanghai Banking Association. **FA**



Comprehensive Anti-Money Laundering Solution

Sanctions and PEP Screening

Ultimate Beneficial Owner Due Diligence and Screening

Real-time Transaction Screening

Transaction Monitoring

Multi-language Capability

FinScan's exceptional accuracy

- ✔ Minimizes False Positives
- ✔ Reduces Exposure to Risk

**See for yourself why FinScan is the trusted solution
for the world's leading organizations.**

Contact info@innovativesystems.com for more information.

www.finscan.com

Congratulations to you!

15 YEARS AND COUNTING...



As you can see, we are celebrating 15 years of *ACAMS Today*. To thrive and be relevant to the ever-changing world of money laundering prevention, we had to be cognizant of how “AML” is now the coverage of the movement of illicit funds for a vast array of crimes such as elder abuse, drug and human trafficking, terrorist financing and now cyber-enabled crime. Our members who comprise the lion share of the global AML community have been generous with their expertise, vision and time to assist us with providing the needed articles, interviews and themes to stay ahead of all of the issues that demand our focus. In addition, the expansion of AML to the breadth of entities beyond traditional banking is essential to the ACAMS community and, once again, our members have made sure we cover the areas of challenge in those industries or agencies.

So, in a word, “Thank you!”

ACAMS Today is such an important tool for the AML professional because of the legions of volunteers and our Editorial Committee members who identify topics, authors and categories of coverage and have made possible the many awards *ACAMS Today* has received. Our community believes that we benefit from sharing ideas, best practices and some criticisms with each other and publicly and hopefully, you agree that *ACAMS Today* has the same mission.

A look back

Of course “look-backs” is a pejorative term in AML, but for our purposes let us take a brief look-back at 15 years since *ACAMS Today* launched.

In the first few years after the horrific attacks of 9/11, AML in the U.S. centered on the implementation of the USA PATRIOT Act and the accompanying regulatory obligations that resulted from that comprehensive law.

Then we witnessed a major global reaction to the Bank Secrecy Act (BSA) violations by Riggs Bank in Washington, D.C. Due to Riggs, which no longer exists, the AML community became familiar with the term politically exposed persons (PEPs). At first PEPs were only foreign political figures and those connected to them, but today we are tasked with creating proper due diligence responses to domestic PEPs as well.


In the intervening years, enforcement actions came with dramatically high penalties and there is clear evidence of the issuances of many more formal regulatory criticisms. Government supervisors have indicated that the culture of compliance needed more emphasis and the term “risk-based approach” was bandied about even if most believe it does not actually exist.

I would suggest that another major outcome of the past 15 years is the priority placed on the work of the Financial Action Task Force (FATF) by the AML community as a training tool. FATF has been here since 1989

but the mutual evaluations and the excellent reports and typologies have made their work more directly relevant than it was during the first decade of their existence.

Since 2002, AML has grown to cover gaming, financial technology firms, the explosion of data and the need to perform a robust risk assessment. *ACAMS Today* has responded to these challenges (and ACAMS has created a Risk Assessment tool that our members asked for) by seeking authors who could take the mystery out of these new areas and provide practical advice on compliance and related responsibilities.

Finally, the mission of ACAMS has always been to recognize that AML is a community of many law enforcement, regulators, bankers, vendors, advisors and the other many parts of an “industry” that exists to protect and defend society from those that prey on innocent victims through the movement of monies.

You will see evidence of that mission in the articles from this edition and the previous 15 years. We are proud to offer this publication and the accompanying website to improve our community and we thank you for your ongoing commitment to this worthy cause. 

A handwritten signature in black ink, reading "John J. Byrne". The signature is fluid and cursive.

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

An integrated approach to AML can help establish a culture of compliance.



Transaction Monitoring



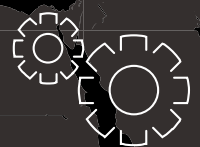
Customer Due Diligence



Currency Transaction Reporting



Watch List Filtering



Case Management

Meet our experts in person:

- [ACAMS moneylaundering.com](http://ACAMS.moneylaundering.com)
April 3-5, 2017 / Hollywood, FL
Booth #100
- [ACAMS 5th Annual AML Risk Management Conference](#)
June 9, 2017 / New York, NY
- [ACAMS 16th Annual AML & Financial Crime Conference](#)
September 25-27, 2017 / Las Vegas, NV

Email info@niceactimize.com to set up a meeting at any of these shows

THE AML RISK PUZZLE

—What does **AML risk** really mean?

If you look up the word “risk” in the dictionary, you will find that it means “exposure to the chance of injury or loss, a hazard or dangerous chance.” This is a very broad definition. From a practical standpoint, risk can be seen as a function of three factors: threat, vulnerability and consequence. In practice, it is difficult to drill down to the meaning of even these specific terms. You throw the term “anti-money laundering (AML)” in front of the word “risk” and it becomes even more confusing.





“A threat is a person or group of people, object or activity with the potential to cause harm.”¹ In the AML “context, this includes criminals, terrorist groups and their facilitators.”² Threat is the factor related to risk that should serve as an essential starting point in developing an understanding of AML risk.

So, what does AML risk really mean? As loose and broad as AML risk is defined, it is still a matter of interpretation—hopefully based on facts and circumstances. There is no standard set of controls, no “right way” to assess risk and no universally acceptable risk tolerance. But, as a banker, we hear how regulators want us to define AML risk; we hear how the Financial Crimes Enforcement Network wants us to view risk; we hear how law enforcement defines AML risk and we hear how our individual lines of business, management and board all define

AML risk. As BSA professionals we have to sit back and ask ourselves, “How are we going to solve the puzzle as to what AML risk is going to mean at our institution?”

Understanding AML risk throughout the organization

One of the biggest problems that we face at my organization is that not all of our business line representatives fully understand AML risk and how it applies to their respective products and services. The communication we have with them sometimes seems to be one sided. We do all the talking and literally have to pull information out of

¹ “National Money Laundering and Terrorist Financing Risk Assessment,” FATE, February 2013, http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

² Ibid.

THREAT IS THE FACTOR RELATED TO RISK THAT SHOULD SERVE AS AN ESSENTIAL STARTING POINT IN DEVELOPING AN UNDERSTANDING OF AML RISK

our various business lines that is useful and meaningful. This is because they get caught up with what their unit means to customers and the bottom line, which we all know is important, but not necessarily relevant to AML. When a business line representative calls me to ask a question as it relates to BSA/AML, the first sentence is always, “I have a very good customer who has a lot of money at our bank.” That is great for the bank, of course, but it does not really mean anything for AML risk. It shows that the caller does not understand how their customer and the product or service that they are using could potentially have AML risk associated with it.

Failure to understand these risks can lead to faulty controls and increased risk. For example, when my AML group called our ACH department about a particular customer’s activity, they responded with, “We risk rated their financial information and they are a good credit risk.” Well, from a BSA/AML perspective, this does not also mean they are a good AML risk. What we want to know is how this customer is moving money, why are they moving this money, where did they get the money and whether their activity corresponds with the activity that is expected of this customer. I knew one day that I finally had someone understand the true meaning of AML risk when an employee from our operations area called and said, “We have a customer who deals in used batteries overseas. Their invoices indicate that they are selling these used batteries at extremely high prices. I cannot imagine that used batteries have that kind of resale value. They started out sending around \$100,000 in wires a month; six months later, they were sending \$2 million and now they are up to \$6 million.” Finally, that aha moment where the elusive AML risk is understood outside of the AML group!

The goal of AML professionals is to reduce the bank’s vulnerability to both ML and TF. Business lines are looking to ensure that the customer will not incur a financial loss for the bank. It is our responsibility to bridge the gap between these two distinct perspectives, by ensuring an understanding of ML and TF and the risks that these activities pose to our

institution. This understanding of AML risk is required to determine what controls may assist in combating these risks and what steps need to be taken if the risk cannot be mitigated.

The challenges of risk-based compliance programs

So, let us talk about the challenges that we face in trying to develop and maintain a risk-based compliance program. Have you ever called someone, such as a banker you respect or your regulator, to get advice or ask for guidance and you simply are told, “Well, is it risk based?” And then you ask yourself, “What does that mean? How do we measure, monitor, control and ultimately report on risk? Also, how do we best work with our business lines, our regulators and law enforcement? Do we need to understand risk?”

THE GOAL OF AML PROFESSIONALS IS TO REDUCE THE BANK’S VULNERABILITY TO BOTH MONEY LAUNDERING AND TERRORIST FINANCING

AML presents a variety of risks from multiple perspectives (i.e., reputational and operational) and from multiple sources (i.e., products, customers and geographies) that must be identified proactively, evaluated and managed. Those are three words that from a financial institution perspective should help direct our efforts in identifying what risk means to our own institution. To do this, we must proactively engage our business lines, our regulator and our local law enforcement. However, doing so can sometimes be a challenge.

Business lines

Let us start with our business lines. There is a huge language barrier here, which is a challenge in and of itself. Getting business lines to see AML risk as it relates to the service or product their business is offering and how ML or TF can flow through it is an education challenge. As BSA professionals, we need to get into their particular line of business to understand and be able to discuss how AML impacts them. We should meet with business line representatives regularly to discuss what is currently going on in their world and what they see their customers doing. Information from these meetings is absolutely essential to solving the risk puzzle.

Regulators

Next are our regulators. Are both of us always on the same page as to how AML risks actually affect our institution? In some areas, maybe yes; and in some, maybe no. We need to discuss the risks we see at our institution with our regulator and ask for feedback well before an examination. This is extremely important. We see them every year anyway. Why not include them? They will be reviewing our risk decisions eventually, and doing so early affords an opportunity to re-evaluate based on their feedback. They are in a position to provide views on whether a particular risk is being adequately identified and managed. For example, we recently began offering online account openings, which I dreaded for years but knew we could only hold the bank off for so long. So, in the initial stages of our planning, I reached out to one of our regulators for examples of risks and best practices they have seen. This proved to be a beneficial and a meaningful discussion—the results of which were communicated back to the affected business lines. The discussion helped everyone understand the role BSA would play in the new offering.

Law enforcement

Lastly is law enforcement. They want a lot from bankers, but sometimes it is hard to see what we receive in return. We file suspicious activity reports (SARs), they ask for more documentation and then maybe three to five years down the road we see an article in the newspaper where our SAR customer has been arrested or indicted. Do not let this discourage you. Try to meet with law enforcement to get information that may inform your AML risk scenario. Recently we have been successful in

meeting local law enforcement on a periodic basis in some of our markets. Law enforcement can provide information on specific cases involving your footprint or customers, relevant statistics on AML investigations, prosecutions and convictions, as well as assets seized and new trends and risks detected through their investigations. We talk about what information they like to see us report in SARs and how to say it to get their attention. We then communicate that back to our staff to ensure everyone has an understanding for what to be on the lookout.

Successful communication with business lines, regulators and law enforcement goes a long way in solving AML risk questions and issues. The results of these conversations also help us to develop our education and internal training about the risk assessment, which is key to an effective risk assessment implementation. By strengthening all three of these avenues, you are helping to solve the risk puzzle.

The risk assessment process

From a small bank perspective, we really do not have enough resources to hire consultants or purchase expensive software. So, we use what we have at our fingertips to help us determine what risk factors to look for within our business lines. The first place I go to is the FFIEC BSA/AML Examination Manual. I find that the expanded sections in the Manual provide guidance and discussion on specific lines of business, products and customers that may present unique challenges and exposures that we need to consider.

In some cases, each section of the Manual also gives some example-controls that can be put into place to mitigate that risk. One that comes to mind is that the bank should have a policy that requires “the processor to identify its major customers by providing information such as the merchant’s name, principal business activity, geographic location and transaction volume.”³ Another is monitoring the charge-back history, including rates of return for ACH debit transactions and remotely created checks. This type of information can help you not only create your risk assessment, but also help you train and educate your lines of business to understand their AML risk. Once trained, they should then be able to gather the information, so they can report back to you.

BSA Action Team

At our institution, we formed a BSA Action Team that meets quarterly. The BSA Action Team is comprised of key individuals from both the BSA group and each line of business. Each line of business is to report on what is going on in their area as it relates to BSA. Using the example again on third-party payment processors, the line of business owner would report any major additions to processors, any reviews performed on the processor’s major customers, if the rates of return have increased and what types of returns we are seeing (i.e., are they just normal account closures or are there patterns of high volumes that could indicate fraud or money laundering).

I find that asking each business line to come prepared to discuss the AML risk and trends in their area to the BSA Action Team makes them really want to understand what to present. Another thing I tell them is when we are being examined, the regulators like to speak with some of the retail and operations departments. I ask them to take note of what they are being asked, the information that they are providing to them and to relay this information to the Action Team during our quarterly calls. All of this helps us to manage our risk on an ongoing basis.

The first step to pinpointing your AML risk is to identify your particular services, the customers that you bank, products that you are currently offering and geographies that you impact. Then use those sections of the Manual to help you identify and evaluate so you can train and involve those lines. In addition to the Manual, there are specific press releases and communications that the regulators publish.

One that comes to mind was on remote deposit capture. That issuance went into detail about the various risks associated with this service. It was a great foundation for us to build our risk assessment and for communicating any issues we may have seen or experienced. It showed that particular line of business what their concerns should be.

Another way to evaluate risk is “to determine whether ML or TF risks should be assessed separately or together. Factors associated with TF that might need to be considered may be very different from those associated with ML. Funds used for financing terrorist activities may be derived from criminal activity or legal sources. In addition, a key focus in combating TF is on preventing future terrorist acts from occurring, whereas with combating ML the criminal activity has already taken place. Another difference is that transactions associated with TF may be conducted in very small amounts, which when not viewed in the terrorist financing context, could be the very transactions that are frequently considered to involve minimal ML risk.”⁴ This is an example of how the design of your monitoring program matters and how you should tailor it to the risk you are monitoring.

Key risk indicators

Yet another way of identifying and analyzing your risks are by looking at trends known as key risk indicators (KRIs). Do you have any KRIs for BSA?

- For example, how many currency transaction reports do you file each quarter? Is that number stagnant or does it increase each quarter? If it increases each quarter, then by how much and is that an indication that your customer’s cash activity is on the rise?
- Another one is how much international activity do you generate in wires or IATs? Is that number increasing, decreasing, or flat? If it is increasing, then you need to know what is going on with those

³ “Third Party Payment Processors—Overview,” FFIEC, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm

⁴ “National Money Laundering and Terrorist Financing Risk Assessment,” FATF, February 2013, http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

customers who send the majority of your wires or send wires to your identified high-risk countries.

- How many high-risk customers do you have and how many in certain industries? If your high-risk customers continue to increase, what is happening to your customer base?

These are examples of types of KRIs to consider and monitor on a regular basis in order to manage your institution's risks. This is why you need to involve your various business lines who can help put the pieces of the risk puzzle together.

The risk assessment

Now that we have identified and evaluated our AML risk, it is time to effectively manage it by preparing that dreaded written risk assessment. But by this point it really is not that hard. Everything that you just identified is placed in the specific risk categories (i.e., products, services, customers, entities, transactions and geographic locations), aggregated and then evaluated. You document your analysis of the data identified to better assess the risk within these categories and the controls being utilized and then you should be ready to address and document the varying degrees of risk associated with each. The risk assessment should be your road map. Anyone reading it, especially examiners, should know all about you and where and what your defined risks are.

One important thing to note is that your risk assessment should not be stagnant. As you continue to meet and review your lines of business, communicate with law enforcement and have continuing conversations with your regulator, you must remember to update your risk assessment.

Best practices for communicating risk

Once you have completed the risk assessment, communicating the results is important to its success.

Internal communication

Here is what we do: We share the completed risk assessment with all business lines across the bank, as well as the board of directors, management and staff. We do this to build organizational

awareness, knowledge and understanding. Your AML risks should be in a concise and organized presentation.

For communication to your lines of business, it is a good idea to provide them with handouts, emails, online training courses—but these should only be supplements. However, nothing is better than getting everyone together and having meaningful conversations about the risk assessment results. Whether it be one-on-one with each unit or in a group setting, it is important to us to ensure that everyone understands their role, their risks, controls and risk appetite of the organization.

Those who work the front line—tellers, loan officers, brokers, customer service representatives and such—perform a critical, but often undervalued, role in managing AML control processes. Because front-line employees have the most direct interaction with customers, they are a bank's first line of defense in identifying and preventing financial crime. It is critical, then, that the AML risk assessment, compliance training and communication they receive is effective.

In addition, it is very important that your risk assessment, ongoing monitoring, trends and risk profile be communicated to your senior management and board. This allows them to be continually involved and to help set the tone from the top as it relates to the bank's risk tolerance.

External communication

As you are aware, law enforcement is key in the fight against ML and TF. Our information continues to play an integral role in law enforcement investigations at both the federal and state levels. Law enforcement uses BSA reporting to identify significant relationships, patterns and trends. This reporting reveals the relationships between illicit customers and their financing networks, which enables law enforcement to target them, use forfeiture and sanctions to disrupt their ability to operate and finance their illicit activity. The same information can also help your institution protect itself and aid law enforcement in protecting your institution from criminals. The importance of this from a communication perspective institutes a culture of compliance at a financial institution ensuring that

ONE IMPORTANT THING TO NOTE IS THAT YOUR RISK ASSESSMENT SHOULD NOT BE STAGNANT

personnel at all levels understand the purpose and usefulness of BSA reporting, helping us to further review the risks that these types of customers bring to our own institution.

Risk assessments are shared with examiners during the examination process. During the exam, recommendations are considered for incorporation into the assessment. It is an opportunity for you to tell your story. However, it is very important that we have ongoing communications outside of the exam. There should also be regularly scheduled calls with your supervisory regulator, and significant risk events or concerns should be discussed. When there is an interesting situation that comes up or if we are trying to make a decision on whether or not to file a SAR, we should reach out to our supervisory contacts to discuss the situation. I have contacted our regulators when I have received a communication from Treasury, I have reached out about filing marijuana-related SARs, and I have asked for guidance on rejected IAT transactions. Communicating often helps us make good decisions and helps our regulator keep abreast on what we face daily.

Conclusion

It is no small task to understand AML risk. You must develop both internal and external partners to help you along this road. If you work with your partners and learn from each other, you may just be able to solve the ever-elusive AML risk puzzle. **A**

*Lisa Varner, senior risk management officer, United Bankshares, Inc., Pittsburgh, PA, USA,
lisa.varner@bankwithunited.com*

ACAMS | Risk Assessment[®]

acamsriskassessment.com

MEASURE, UNDERSTAND & EXPLAIN YOUR MONEY LAUNDERING RISKS

This first-of-its-kind solution helps your institution:

- Identify risks within and across all lines of business
- Mitigate risk by filling in the gaps in your detection and prevention controls
- Present trusted reports that are up-to-par with the latest global regulation and guidance
- Clearly communicate risk to all stakeholders through standardized and automated presentation-ready reports



Schedule a product demo: riskassessment@acams.org

ARE COMPLIANCE TESTING FUNCTIONS ALIGNED OR **OVERLAPPING?**



In most organizations, whenever something goes wrong, the first question usually is, “Why was it not uncovered by the regulators, auditors, or the organization’s own assurance or testing teams?” Audit, independent testing and assurance are concepts that have permeated the business practices of many organizations for decades, if not centuries. Yet, their meaning and significance have changed substantially throughout the years, most notably within the financial services sector, which has experienced special influence from supervisory standards introduced in response to the 2008 financial crisis.

For large banking organizations, the initial driving force behind the evolving connotation of “compliance testing” was SR 08-8, a supervisory letter issued by the Board of Governors of the Federal Reserve System¹ back in 2008, which detailed regulatory expectations regarding compliance risk management programs, consistent with the guidelines issued by the Basel Committee on Banking Supervision concerning the compliance function in banks. According to both, one of the key pillars of a sound compliance risk management structure consists of compliance monitoring and testing. Fast forward to 2014, the Office of the Comptroller of the Currency (OCC) issued guidelines to strengthen the governance and risk

management practices of large financial institutions,² also known as Heightened Standards, introducing what is today a widely known and accepted concept: the three lines of defense consisting of front line, independent risk management and internal audit.

In terms of testing, much clarity seems to exist in regards to roles and responsibilities of internal audit, the third line of defense: independence, board’s audit committee, audit plan, identification of root cause, issue resolution, etc. In contrast, there is obscurity in the realm of the first and second lines. Coordinating the testing responsibilities efficiently without overlapping is a real challenge. Because compliance structures within the first line have historically been the

least developed over the years (focus on business), the response by some institutions to the lack of tangible guidance and increased scrutiny by regulators in regards to testing has been to create within the second line more structured testing programs, more sophisticated methodologies and more inflated teams. On one hand, the more an institution performs tests, the more chances it has to uncover mistakes, issues and

ONE OF THE KEY PILLARS OF
A SOUND COMPLIANCE RISK
MANAGEMENT STRUCTURE
CONSISTS OF COMPLIANCE
MONITORING AND TESTING

¹ FRB Supervisory Letter SR 08-8 / CA 08-11, October 16, 2008, <https://www.federalreserve.gov/boarddocs/srletters/2008/sr0808.htm>

² Office of the Comptroller of the Currency 12 CFR Parts 30 and 170; [Docket ID OCC-2014-001]; RIN 1557-AD78, September 2, 2014, <https://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-117a.pdf>

gaps. On the other hand, since testing is a key component of a risk management program, the true and self-definition of risk management cannot be ignored: managing risks, which means not every mistake, issue or gap needs to be uncovered. An army of testers is not the solution; in contrast, compliance testing should be conducted on a risk-based priority schedule and testing functions within each of the three lines of defense need to be aligned and not overlap.

This lack of definition and guidance also leads to a variety of misinterpretations and sometimes institutions are left in a situation where groups from each line of defense are making a case that is more convenient for them. There are often situations where the first line is looking up to the second for the development and deployment of assurance activities while at the same time the second line is turning to the first to leverage what they believe risk owners should be testing. Historically, not only smaller organizations but also large banks have been staffing and tasking the second line of defense to essentially identify and stop compliance irregularities. As previously mentioned, only recently has this accountability been shared with the first line, so it is still common nowadays to find large compliance testing teams within the second line of defense and no self-testing at all within the first. Resource allocation goes hand in hand with the size and complexity of each department within an organization and may be perceived as a reflection of their importance. In some situations, letting go of resources by the second line in lieu of the need for the first to execute testing activities

**THE ULTIMATE GOAL IS TO HAVE
A SUCCESSFUL COMPLIANCE
PROGRAM WITH THE LEAST
AMOUNT OF REGULATORY ISSUES**

may be a challenge. Similarly, shifting the roles of business centric human resources within the first line to essentially become their colleague's 'police' is audacious, to say the least. So, what is the right way to go about it? Who needs to test what? Is there an optimal and cost-effective way to handle compliance testing programs?

In order to answer these questions, let us begin by examining the testing's intended result. The ultimate goal is to have a successful compliance program with the least amount of regulatory issues. Therefore, the 'burden' should be absolutely split between the three lines in a manner where one feeds off the other: from the day-to-day quality control within the first line to an assessment of the design and operating effectiveness by the second, to the widest scope within the third. If it is not well designed, the execution could become repetitive and the outcomes could conflict with each other, resulting in inefficiency at high costs. Staffing levels should be directly proportionate to the needs of each activity being performed

by the three lines. Day-to-day quality control relates to ongoing repetitive tasks that are operational and volume based. This generally translates into a higher headcount. Conversely, in order to assess the design and operating effectiveness of a compliance program, the second line needs to be staffed with a smaller group of subject-matter experts who will develop and apply more sophisticated testing techniques in order to assure the program, framework and structure are working as intended. Internal audit is an even smaller subset and as per their own practice standards, audit teams are usually staffed based on the collective knowledge concept, whereby the audit group combined has the associated skills and competencies necessary to complete planned audits and support the audit function as it evolves. Testing functions within the first, second and third lines must be complementary of each other and as a whole protect the institution against unknown gaps and shortcomings on compliance coverage.

As previously established, a general consensus seems to exist in regards to the roles and responsibilities of the third line of defense. However, there is ambiguity in terms of the first and second lines when it comes to testing. Due to the nature, size and complexity of each financial institution, organizations take different approaches when structuring and staffing each of these groups from a compliance testing perspective.

Given the premise that these functions should not be overlapping, one way to minimize ambiguity between the roles of first and second lines in terms of compliance testing within financial institutions is by employing the

FROM A COMPLIANCE PERSPECTIVE, MATURITY IS REACHED WHEN ORGANIZATIONS FULLY UNDERSTAND THE ROLES, RESPONSIBILITIES AND ACCOUNTABILITIES OF THE THREE LINES OF DEFENSE

concepts long used by the technology and manufacturing industries. These concepts include clearly distinguishing quality assurance (QA) from testing and how these concepts, though closely related, should be performed by different groups. In simple terms, testing is usually defined as the process of executing a task with the intent of finding defects. Different from the QA team, testers are expected to operate under the assumption that breaches exist and must be uncovered. They function in such a way that they expect to find problems, not just to confirm that it is possible for everything to work fine given a set framework. On the other hand, QA is a set of activities designed to assess whether the process is adequate to ensure a program or function will meet its objectives. QA is less focused on breaking processes or activities apart and finding problems; rather, it is about confirming that it is possible to make the process or activity work under a given set of conditions.

Different concepts surrounding different roles and objectives instinctively call for separate groups of responsibility. The notion of establishing two distinct groups is nowadays becoming better accepted, especially within large banks, although controversy can arise around where testing and assurance activities reside. In line with OCC's Heightened Standards, which indicates that risks associated with the front-line units' activities should be effectively identified, measured, monitored, and controlled consistent with the bank's risk appetite statement, concentration risk limits, and the bank's policies, large banking organizations should be tasking their first lines of defense with testing. The front line owns regulatory

control of its products, services, and operations and should therefore have built-in procedures, controls and testing that ensure that regulatory requirements are followed at all times.

Once the responsibilities and objectives of the first and third lines are defined, the second line's role is then a given. QA should be assigned to the second line of defense, which works closely with, but independently from the front line to ensure that the business has appropriately identified, measured, assessed and managed the risk in the business. Their work is not about "check-the-box," rules-based testing processes, which do not provide adequate coverage over the design of the compliance program as a whole—policies, procedures, internal controls and training. In contrast, QA within the second line of defense, requires a strong understanding of end-to-end business processes and controls and an assessment of their adequacy given applicable regulatory requirements. This understanding helps the overall compliance program as it exposes the full range of interconnected processes, the hand-offs and dependence between the various areas which may be structured in silos, but most likely place reliance on one another when it comes to compliance controls. For instance, a QA focused on Office of Foreign Assets Control (OFAC) compliance for a specific line of business could yield skewed results if testing were to be purely designed to verify whether or not the customer is/was part of the Specially Designated Nationals list. Conversely, an end-to-end process review could unveil a breakdown of hand-offs between the roles of customer onboarding personnel and

back-office operations, such as a time lag between onboarding and screening, non-screening of certain individuals and terminologies, or use of outdated lists. In this case, even though the ultimate result indicates a non-violation of OFAC requirements, inappropriate execution of established processes could expose the institution to compliance risks. A comprehensive end-to-end process review would uncover these deficiencies.

In summary, as organizations mature, proper testing and QA approaches will be implemented by management as a matter of practice. From a compliance perspective, maturity is reached when organizations fully understand the roles, responsibilities and accountabilities of the three lines of defense and utilize those concepts as a way to assess the strength of the assurances provided by each group. First-line testing is about detecting and finding errors to ensure quality. The second line is about preventing errors by analyzing existing programs and frameworks in order to assure quality. The third line must be independent of all areas to safeguard objectivity. Together, the three lines help the organization achieve responsible, effective and sustainable compliance risk management. **TA**

Alba Kiihl, CAMS-Audit, vice president BSA/AML testing, Boston, MA, USA, albakiihl@hotmail.com

The views in this article are those of the author and do not necessarily represent those of any organization or company.



CYBER SECURITY: FAKE NEWS, BOTS, BOTNETS AND CLICK FRAUD

The *New York Times*¹ recently reported on an example of how fake news can reach beyond celebrities and political figures to the reputation of private citizens and their businesses. Specifically, the fake news example alleged irresponsibly that a Washington, D.C. pizzeria was being used as a front for a child sex trafficking operation. A major catastrophe was averted afterwards, when law enforcement arrested a man who entered the pizzeria to investigate the hoax armed with an assault rifle.²

This article focuses on challenges that fake news presents to financial crimes investigators and on examples of cybersecurity threats that may accompany fake news through bots, botnets and click fraud, given the recent advisory to financial institutions on cyber-events and cyber-enabled crime from the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN),³ which provides suspicious activity report (SAR) filing examples and a frequently asked questions document.⁴

Fake news

Disinformation designed to deceive or obscure the truth has long been a part of the competitive landscape. Yet, recent headlines about Google, Twitter and Facebook efforts to curb profits derived from fake news⁵ raise significant concerns for financial crimes investigations.

Fake news makes it harder to rely on traditional news and social media for negative news. Financial crimes investigators should always be on the

lookout for fraudulent misinformation, hoaxes and satire that make it harder to find reliable adverse media. Healthy skepticism is appropriate when reviewing search results, such as negative reviews⁶ about individuals or businesses, or positive reviews that are withheld from public view to manufacture demand for online reputation management software and services.⁷

It is best to read beyond headlines⁸ and to be skeptical of online news from unfamiliar news outlets. A website registrant's identity can be investigated by typing the domain name into WHOIS.net, and then repeating this step using the registrar's WHOIS Lookup.

In addition, pay close attention to news website addresses when typing into browsers or selecting from search results. For example, cnn.com may be intended when cnn.om is typed instead due to a typographical error. A fake news website could exist at the cnn.om web address, since .om is the Internet country code top-level domain for Oman. An online list of reportedly malicious .om websites includes cnn.om.⁹

Typosquatting websites may disregard the intellectual property¹⁰ and unfair competition¹¹ protections of legitimate news outlets, and deliver fake news¹² and malware¹³ to Internet users.

The author's identity and reputation for accurate reporting should be investigated, along with the presence of reliable news sources and the accuracy of facts, quotes and publication dates. News blogs and articles may be ghost-written, as some authors may be using online reputation management services to bury unwanted search results by positioning themselves as industry thought leaders.¹⁴ Both derogatory and favorable news about individuals or businesses should be corroborated for accuracy, completeness and relevance.

Photographs should also be checked. Origins and previous postings of photographs can be verified through reverse image search by dragging the photograph into web-based tools like TinEye¹⁵ or Google Images.¹⁶ Photograph date-, time- and location-tracking data can be

¹ Pui-Wing Tam, "Anti-Clinton Fake News Casts Pizzeria as Front for Crime," *The New York Times*, November 22, 2016, <http://www.nytimes.com/2016/11/22/technology/anti-clinton-fake-news-casts-pizzeria-as-front-for-crime.html>

² Keith L. Alexander, Susan Svrluga, "I am sure he is sorry for any heartaches he has caused, mother of alleged 'Pizzagate' gunman says," *The Washington Post*, December 12, 2016, https://www.washingtonpost.com/local/public-safety/i-am-sure-he-is-sorry-for-any-heartaches-he-has-caused-mother-of-alleged-pizzagate-gunman-says/2016/12/12/ac6f9068-c083-11e6-afd9-f038f753dc29_story.html?utm_term=.50c512a5f409

³ "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

⁴ "Frequently Asked Questions (FAQs)," *United States Department of the Treasury—Financial Crimes Enforcement Network*, October 25, 2016, https://www.fincen.gov/sites/default/files/shared/FAQ_Cyber_Threats_508_FINAL.PDF

⁵ Abby Ohlheimer, "This is how Facebook's fake-news writers make money," *The Washington Post*, November 18, 2016, <https://www.washingtonpost.com/news/the-intersect/wp/2016/11/18/this-is-how-the-internets-fake-news-writers-make-money/>

⁶ "Lawsuit over negative Yelp review heads to Calif. Supreme Court," *CBS News*, September 22, 2016, <http://www.cbsnews.com/news/lawsuit-over-negative-yelp-review-california-supreme-court/>

⁷ Cheryl Conner, "The Dark Side of Reputation Management: How It Affects Your Business," *Forbes*, May 9, 2013, <http://www.forbes.com/sites/cherylsnappconner/2013/05/09/the-dark-side-of-reputation-management-how-it-affects-your-business/#1f572fcc4b89>

⁸ Nick Robins-Early, "How to Recognize a Fake News Story," *The Huffington Post*, November 22, 2016, http://www.huffingtonpost.com/entry/fake-news-guide-facebook_us_5831c6aae4b058ce7aaba169

⁹ Endgame—List of malicious .om sites, *Pastebin*, March 11, 2016, <http://pastebin.com/q2WCuw6K>

¹⁰ William Needle, "Chapter No. 4.3 Trademark Primer," *Concept Foundation, PIPRA, FIOCRUZ and bioDevelopments-Int. Institute*, <http://www.iphandbook.org/handbook/ch04/p03/>

¹¹ Florina Yezril, "Somewhere Beyond the ©: Copyright and Web Design," *NYU Journal of Intellectual Property & Entertainment Law*, December 17, 2015, <http://jipel.law.nyu.edu/vol-5-no-1-2-yezril/>

¹² Elizabeth Weise, "Hackers use typosquatting to dupe the unwary with fake news, sites," *USA Today*, December 1, 2016, <http://www.usatoday.com/story/tech/news/2016/12/01/hackers-use-typo-squatting-lure-unwary-url-hijacking/94683460/>

¹³ Lily Hay Newman, "Be Careful. Mistyping a Website URL Could Expose You to Malware," *Slate*, March 17, 2016, http://www.slate.com/blogs/future_tense/2016/03/17/hackers_use_om_urls_for_typosquatting_malware_attacks.html

¹⁴ *BrandYourself Concierge Service*, <https://brandyourself.com/info/about/howItWorks/concierge>

¹⁵ *TinEye*, <http://www.tineye.com>

¹⁶ *Google Images*, <https://images.google.com>

verified using web-based metadata verification tools, like Metapicz¹⁷ and Jeffrey Friedl's Image Metadata Viewer.¹⁸

The absence of photograph editing can be confirmed using web-based services like Izitru,¹⁹ which also certifies photographs that it deems to be authentic. Such certification may be of special value to auction websites and other online sellers with photographs that buyers rely on before purchasing goods and services.

Fake news may expose Internet users to cybersecurity risks through online searches, traditional news sources and social media. Be on the lookout for malware disguised as news and other announcements, including browser updates,²⁰ security patches²¹ and software updates.²²

Detecting disguised malware requires consistent attention to detail and context. Some malware may be easy to spot, such as update pop-ups with typographical errors, unprofessional English, or logos that do not match

trademarks. Be wary of updates that appeal to emotions or a sense of urgency. If update requests appear unexpectedly, check instead for downloads on the software vendor's website. The FBI has warned about malware that appears as software update pop-ups when using public hotspots or hotel Internet services. Malware may appear as fake software updates to users who browse free media websites or download free software. Security software should be set to auto-update, run at all times and protect endpoints, such as laptops and mobile devices. Auto-updates should be checked intermittently, since malware can hijack auto-updates.²³

Cybercriminals may use email,²⁴ link clicks to news articles²⁵ and advertisements,²⁶ and word searches (including personal name searches)²⁷ to load malware, spyware and spam on computers, lure users to malicious websites, and report keystrokes and online activities. Such reporting of keystrokes

and online activities may impact SAR confidentiality that is required by U.S. federal law.²⁸

Bots and botnets

Automated computer programs, known as bots, are frequently used to spread fake news.²⁹

Not all bots are created equal. An example of a good bot is Googlebot, Google's web crawling bot used to discover new and updated Internet webpages to be added to its search index.³⁰

Unfortunately, bots have a bad reputation because cybercriminals often use them to control an infected computer for nefarious purposes. Online companies face greater challenges distinguishing real customers from bad bots that can steal website content through web scraping,³¹ commit click fraud,³² and hijack user accounts.³³ On online gambling websites, bots compete against human players, contrary to the

¹⁷ Metapicz, <http://metapicz.com>

¹⁸ Jeffrey Friedl's Image Metadata Viewer, <http://exif.regex.info/exif.cgi>

¹⁹ Izitru, <http://www.izitru.com>

²⁰ Larry Loeb, "Firefox Malware Poses as Browser Update," *Security Intelligence*, July 11, 2016, <https://securityintelligence.com/news/firefox-malware-poses-as-browser-update/>

²¹ Mark Jones, "Top Story: Watch out! Malware disguised as Microsoft security update," *Komando.com*, October 29, 2016, <http://www.komando.com/happening-now/378364/watch-out-microsoft-security-update-disguised-as-malware/all>

²² "Keep getting fake Adobe update popup," *Adobe*, September 7, 2016, <https://forums.adobe.com/thread/2205736>

²³ "Is That Software Update Actually Malware?," *ZoneAlarm*, March 11, 2015, <http://www.zonealarm.com/blog/2015/03/software-update-malware/>

²⁴ Elizabeth Shim, "South Korea police warns of malware in emails about Park Geun-hye," *United Press International*, November 23, 2016, http://www.upi.com/Top_News/World-News/2016/11/23/South-Korea-police-warns-of-malware-in-emails-about-Park-Geun-hye/7101479913990/

²⁵ "Visitors of NY Times, BBC, and AOL sites targeted by malware," *Lavasoft*, March 17, 2016, <http://www.lavasoft.com/mylavasoft/company/blog/visitors-of-ny-times-bbc-and-aol-sites-targeted-by-malware>

²⁶ Laura Hautala, "How to avoid getting conned by fake news sites," *CNET*, November 19, 2016, <https://www.cnet.com/how-to/how-to-avoid-getting-conned-by-fake-news-sites/>

²⁷ "Celebrities Bring Us Entertainment, Laughter—and Malware," *Intel Security*, October 4, 2016, <https://securingtomorrow.mcafee.com/business/celebrities-bring-us-entertainment-laughter-malware/>

²⁸ 31 U.S.C. § 5318(g); 31 C.F.R. § 103.18 (U.S. Treasury Department); 12 C.F.R. § 21.11 (U.S. Office of the Comptroller of the Currency); 12 C.F.R. § 563.180 (U.S. Office of Thrift Supervision); 12 C.F.R. §§ 353.1–353.3 (U.S. Federal Deposit Insurance Corporation); 12 C.F.R. § 208.62 (U.S. Federal Reserve Board).

²⁹ John Markoff, "Automated Pro-Trump Bots Overwhelmed Pro-Clinton Messages, Researchers Say," *The New York Times*, November 17, 2016, http://www.nytimes.com/2016/11/18/technology/automated-pro-trump-bots-overwhelmed-pro-clinton-messages-researchers-say.html?_r=0

³⁰ "Googlebot," *Google Search Console Help*, 2016, <https://support.google.com/webmasters/answer/182072?hl=en>

³¹ "The 2016 Economics of Web Scraping Report," *Distil Networks*, 2016, <https://forum.equinix.com/assets/images/files/distil-networks-2016-economics-of-web-scraping.pdf>

³² "The Bot Baseline: Fraud in Digital Advertising—Advertisers will lose \$7.2 billion globally to bots in 2016," *Association of National Advertisers*, 2016, <http://www.ana.net/content/show/id/botfraud-2016>

³³ Bryan Hooi, Hyun Ah Song, Alex Beutel, Neil Shah, Kijung Shin and Christos Faloutsos, "FRAUDAR: Bounding Graph Fraud in the Face of Camouflage," *Carnegie Mellon University*, 2016, <https://www.cs.cmu.edu/~neilshah/research/papers/FRAUDAR.KDD.16.pdf>

SARS HAVE BEEN VITAL IN HELPING THE FBI TO IDENTIFY WIRE TRANSFERS TIED TO BOTNETS OPERATED BY LARGE-SCALE MONEY LAUNDERING OPERATIONS, ACCORDING TO FORMER FINCEN DIRECTOR JENNIFER SHASKY CALVERY

terms of use,³⁴ and circumvent age and identity verification and enhanced customer due diligence.³⁵

The U.S. Congress recently took legislative steps to curb the use of bots that function as online ticket scalpers.³⁶ On December 14, 2016, former President Barack Obama signed the Better Online Ticket Sales (BOTS) Act of 2016, Public Law No: 114-274, which defines the use of bots to purchase tickets in advance and then resell them at a premium as an “unfair and deceptive practice” under the Federal Trade Commission Act.³⁷ Although this law is directed at bots that function as online ticket scalpers, it establishes a foundation for similar efforts to curb the use of bots that harm the online sale of other goods and services.

Bots on one infected computer may be networked with other infected computers through what is called a botnet, which may span globally. Through a botnet, a command and control server can function as a master computer that remotely controls infected computers,

although new variations on this conventional approach are becoming evident.³⁸

Botnets may adversely affect individual Internet users by collecting and sending their personal financial information, such as credit card numbers, bank account details and passwords, to organized criminals and terrorists.³⁹ The FBI has been actively addressing such cybersecurity threats in collaboration with the private sector, U.S. and foreign law enforcement, and other U.S. federal agencies.⁴⁰

SARs have been vital in helping the FBI to identify wire transfers tied to botnets operated by large-scale money laundering operations, according to former FinCEN Director Jennifer Shasky Calverly. This includes the GameOver Zeus botnet associated with losses exceeding \$100 million in the U.S. alone.⁴¹

FBI collaborative efforts have also mitigated DNS Changer, Dridex, Dorkbot, Simda botnets, and other botnet threats that can be used to disseminate viruses

like ransomware. The FBI has collaborated with foreign law enforcement and intelligence agencies through cyber assistant Legal Attachés assigned overseas.⁴²

The Presidential Policy Directive—U.S. Cyber Incident Coordination outlines a public-private collaboration framework to address cybersecurity matters. The Department of Justice, acting through the FBI and the National Cyber Investigative Joint Task Force, is designated as the Federal lead agency for threat response. The Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, is designated as the Federal lead agency for asset response. The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is designated as the Federal lead agency for intelligence support.⁴³

The FBI has been working closely with White Ops, a private sector online fraud prevention firm that recently

³⁴ “Rise of the Machines: How Poker Bots Infiltrated the Online Game,” CardsChat, <https://www.cardschat.com/poker-bots.php#sthash.tSAasWUK.dpuf>

³⁵ “You need to know your customers—remote casinos: Customer due diligence in remote casinos,” *Gambling Commission*, December 2015, <http://www.gamblingcommission.gov.uk/Gambling-sectors/AML/How-to-comply-AML/You-need-to-know-your-customers.aspx>

³⁶ Ray Waddell, “Inside the Music Industry—and Congress’—Fight Against Ticket Bots,” *Billboard*, June 23, 2016, <http://www.billboard.com/articles/business/7416096/ticket-bots-illegal-software-music-stars>

³⁷ Enrolled Bill Text—S.3183—114th Congress (2015-2016): BOTS Act of 2016, *Congress.gov*, <https://www.congress.gov/bill/114th-congress/senate-bill/3183/text>

³⁸ Botnets Today, *Microsoft Security Intelligence Report*, https://www.microsoft.com/security/sir/story/default.aspx#!botnetsection_p2p

³⁹ Joseph Demarest, “Taking Down Botnets,” FBI, July 15, 2014, <https://www.fbi.gov/news/testimony/taking-down-botnets>

⁴⁰ “International Cyber Crime—Iranians Charged with Hacking U.S. Financial Sector,” FBI, March 24, 2016, <https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector>

⁴¹ Prepared Remarks of FinCEN Director Jennifer Shasky Calverly, delivered at the FSSCC-FBIIC joint meeting, *FinCEN*, December 9, 2015, <https://www.fincen.gov/sites/default/files/shared/20151209.pdf>

⁴² “DHS, DOJ Respond to Carper Inquiries on Agencies’ Response to Threat of Ransomware,” *U.S. Senate Committee on Homeland Security & Governmental Affairs*, March 30, 2016, <https://www.hsgac.senate.gov/media/minority-media/dhs-doj-respond-to-carper-inquiries-on-agencies-response-to-threat-of-ransomware>

⁴³ “Presidential Policy Directive—U.S. Cyber Incident Coordination,” *The White House*, July 26, 2016, <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

discovered the Methbot botnet, which is associated with losses exceeding \$180 million.⁴⁴

New provisions of Rule 41 of the Federal Rules of Criminal Procedure went into effect on December 1, 2016. The Electronic Frontier Foundation asserts in part that Rule 41 will now make it easier for law enforcement to obtain search warrants if a computer is part of a botnet, and urges additional safeguards.⁴⁵

Click fraud

Online advertising pay-per-click bot and botnet schemes have presented organized criminals and terrorists with opportunities for money laundering⁴⁶ through click fraud.⁴⁷


For example, click hijacking, also called click jacking, may be associated with

fake news as a lure to social media click fraud.⁴⁸ A botnet linking over 4 million computers in more than 100 countries allowed a group of organized criminals to run click jacking malware that would trick users into clicking on a hidden layer of links or buttons, so that the organized criminals might fraudulently collect over \$14 million in advertising pay-per-click revenue. The Estonian co-conspirators posed as an online advertising firm linked to over a dozen front companies in Cyprus, Denmark, England, Estonia, the Republic of Seychelles, Russia, and the U.S.; one Russian co-conspirator reportedly remains at large.⁴⁹

Click jacking has been used to trick computer users into turning on microphones and cameras without their knowledge. Prevention of click jacking can include updates to Internet

browsers and Flash plugins, along with click jacking detection and prevention software.⁵⁰

The term “click laundering” may be of interest to anti-money laundering/counter-terrorist financing investigators. In 2010, Microsoft popularized the term click laundering to describe another form of click fraud that makes invalid ad clicks appear to originate from legitimate sources.⁵¹ Click laundering attempts to avoid fraud detection systems that have been put in place by the Microsoft adCenter platform to protect online advertisers. The name “click laundering” highlights an analogy to money laundering in that the origin of illegal profits is disguised as legitimate.⁵²

In conclusion, cybersecurity threats that accompany fake news through bots, botnets and click fraud may be reportable in SARs subject to the recent FinCEN advisory, which describes cyber-events, cyber-enabled crimes and cyber-related information, and provides SAR filing examples and a frequently asked questions document. 

CLICK JACKING HAS BEEN USED TO TRICK COMPUTER USERS INTO TURNING ON MICROPHONES AND CAMERAS WITHOUT THEIR KNOWLEDGE

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

⁴⁴ Jose Pagliery, “Russian ‘methbot’ fraud steals \$180 million in online ads,” CNN Tech, December 20, 2016, <http://money.cnn.com/2016/12/20/technology/ad-fraud-online-methbot/>

⁴⁵ Jamie Williams, “Expanded Government Hacking Powers Need Accompanying Safeguards,” *Electronic Frontier Foundation*, December 14, 2016, <https://www.eff.org/deeplinks/2016/12/expanded-government-hacking-powers-need-accompanying-safeguards>

⁴⁶ “Ad Networks: A New Avenue for Money Laundering,” *Trulioo*, October 27, 2015, <https://www.trulioo.com/blog/ad-networks-a-new-avenue-for-money-laundering/>

⁴⁷ “Clicks and impressions—Definition of invalid click activity,” *Google AdSense Help*, <https://support.google.com/adsense/answer/16737?hl=en>

⁴⁸ Susan Hogan, “Internet users falling prey to ‘click-jacking’ schemes,” *WPRI 12 Eyewitness News*, October 20, 2014, <http://wpri.com/2014/10/20/internet-users-falling-prey-to-click-jacking-schemes/>

⁴⁹ “Estonian Cybercriminal Sentenced for Infecting 4 Million Computers In 100 Countries With Malware In Multimillion-Dollar Fraud Scheme,” *United States Department of Justice*, April 26, 2016, <https://www.justice.gov/usao-sdny/pr/estonian-cybercriminal-sentenced-infecting-4-million-computers-100-countries-malware>

⁵⁰ Andy O’Donnell, “How to Protect Yourself From Clickjacking Attacks,” *Lifewire*, October 20, 2016, <https://www.lifewire.com/how-to-protect-yourself-from-clickjacking-attacks-2487178>

⁵¹ Nancy Gohring, “Microsoft Chases ‘Click Laundering,’” *PCWorld*, May 19, 2010, <http://www.pcworld.com/article/196694/article.html>

⁵² Bill Harmon, “Microsoft Adds New Defendant in Click Laundering Lawsuit,” *Microsoft*, December 10, 2010, https://blogs.technet.microsoft.com/microsoft_on_the_issues/2010/12/10/microsoft-adds-new-defendant-in-click-laundering-lawsuit/

Have you done your due diligence on your due diligence service?

YOU'RE ONLY AS STRONG
AS YOUR WEAKEST SOURCE

Dow Jones RiskReports provides essential information from the highest-quality, vetted sources. Customize your risk management and base your biggest decisions on the depth and accuracy of RiskReports.

Visit go.dowjones.com/riskreports



DE-RISKING AND FINANCIAL INCLUSION

Correspondent banking relationships (CBRs) play an essential role in economies around the world, enabling local banks to access overseas products and carry out cross-border transactions. But while such relationships are an important feature of the global banking landscape, they are not set in stone.

Over the last couple of years, correspondent banks have chosen to restrict or terminate their relationships with local banks in a variety of markets. The term “de-risking” has been widely used to describe this phenomenon. However, some believe the term has unhelpful connotations—not least because correspondent banking relationships can be terminated or restricted for many different reasons.

Regardless of the terminology used, it is indisputable that many banks around the world have seen their CBRs terminated, leading to considerable challenges for banks and their customers. It is becoming increasingly clear that this trend is at odds with global goals for financial inclusion and that the withdrawal of services is forcing some customers to make payments using less regulated channels.

Banks may choose to restrict or rationalize their CBRs for a number of reasons. Guidance published by FATF in October 2016 cited supervisory penalties, changes in banks’ financial risk appetites and anti-money laundering (AML) compliance costs as key drivers of de-

risking.¹ Meanwhile, low interest rates have led to shrinking profit margins in correspondent banking—meaning that some banks may welcome the opportunity to exit a line of business, which is now less lucrative than in the past.

In November, following the publication of the FATF guidance, the Basel Committee began a consultation on proposed revisions to its guidelines on the *Sound Management of Risks Related to Money Laundering and Financing of Terrorism*. The consultative document notes, “The clarifications are proposed as the international community has been increasingly concerned about de-risking in correspondent banking, since a decline in the number of correspondent banking relationships may affect the ability to send and receive international payments, or drive some payment flows underground.”²

Impact in the Caribbean

While banks around the world have been affected by the practice of terminating correspondent banking relationships, the impact has been more notable in some regions than in others. Research published in November 2015 by the World Bank found that the Caribbean “seems to be the region most severely

affected” by this trend, with 69 percent of the local/regional banks surveyed reporting a moderate or significant decline in CBRs.³

Correspondent banking relationships are particularly important for the Caribbean, as access to foreign financial markets is otherwise limited. At a global conference on correspondent banking, Gaston Browne, Prime Minister of Antigua and Barbuda, stated that the provision of correspondent banking services is a lifeline to Caribbean economies, “without which the region would be excluded from the global finance and trading system with grave consequences for maintenance of financial stability, economic growth, remittance flows and poverty alleviation.”⁴

Over the last couple of years, the region has seen numerous correspondent banking relationships terminated, restricted or subjected to enhanced due diligence procedures. The decision to end or limit certain relationships may be a legitimate business decision from the point of view of individual correspondent banks. However, with the practice becoming increasingly widespread, local banks affected by this trend may struggle to obtain the relevant services from other banks—

¹ “Correspondent Banking Services,” FATF, October 2016,

<http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf>

² “Consultative Document Guidelines,” Basel Committee on Banking Supervision, November 2016, <https://www.bis.org/bcbs/publ/d389.pdf>

³ “Withdrawal from Correspondent Banking: Where, Why and What to do About it,” World Bank, November 2015, <http://documents.worldbank.org/curated/en/113021467990964789/pdf/101098-revised-PUBLIC-CBR-Report-November-2015.pdf>

⁴ “Prime Minister Gaston Browne on De-Risking and Correspondent Banking,” Discover Montserrat, November 3, 2016, <http://discovermni.com/2016/11/03/prime-minister-gaston-browne-on-de-risking-and-correspondent-banking/>

particularly in markets such as the Caribbean, where correspondent banking services have historically been provided by a very small number of U.S. banks.

The consequences of this trend are considerable. Even if a replacement relationship can be found, banks, which have been de-risked, may still face certain challenges. For one thing, the costs involved in a new relationship may be significantly higher than under previous arrangements. For another, the termination of correspondent banking relationships typically carries a three month notice period—a timeframe which may not be sufficient for local banks to set up a replacement CBR.

Impact for end users

The impact of this trend is being felt unevenly across the Caribbean. Some money services businesses (MSBs) have been affected by having their accounts closed—at least one MSB has reportedly closed a franchise in the region as a result of concerns about de-risking. In some cases, de-risking has also reportedly led to the closure of accounts held by legal professionals and charities.

Where non-profit organizations (NPOs) are concerned, de-risking has impeded lifesaving assistance when charities have been unable to transfer funds to foreign countries, according to a report published by the Charity & Security Network in February 2017. The report makes a number of recommendations to address this issue, such as launching a multi-stakeholder dialogue to address NPO financial access, creating an NPO utility to streamline due diligence for financial institutions and creating a special banking channel to facilitate the movement of funds during humanitarian crises.⁵

Consumers also face significant challenges. People in the Caribbean may need to make payments to the U.S. for numerous reasons, such as importing goods, paying for overseas university education for their children or obtaining medical care. At the same time,

citizens working in the U.S. may wish to send money back to their home countries in order to support their families and cover mortgage payments.

Taken to its extreme, the termination of correspondent banking relationships could have severe consequences across society. If university fees or accommodation costs cannot be paid, young people may be prevented from advancing their education—ultimately becoming a lost resource for the region. If mortgage payments are missed, people may lose their homes. If individuals cannot access essential medical attention, their conditions may worsen, possibly with fatal consequences.

Inevitably, if people are unable to make payments through legitimate channels, they will seek other methods of doing so—whether that means using money remittance services or carrying suitcases full of cash across borders. Unlike the mainstream banking system, such methods can be difficult to track, as well as resulting in greater risks for the individuals concerned. Ironically, the use of less regulated channels can lead to greater opportunities for money laundering and criminal activity—the very thing that stringent AML regulation is intended to prevent.

Seeking solutions

In light of these concerns, efforts are underway to address the challenges associated with de-risking. From diplomatic discussions to the creation of new electronic systems, countries around the world are taking steps to implement new structures and solutions.

In some cases, central banks are taking a more active role in supporting local banks. Some countries are adopting new anti-money laundering/counter-terrorist financing (AML/CTF) legislation in order to address correspondent banks' concerns about risks in the relevant markets. At the same time, there is a greater awareness of the need for effective dialogue between correspondents and respondents in order to increase awareness of both parties' challenges and concerns.

⁵ "Financial Access for U.S. Nonprofits," Charity & Security Network, February 1, 2017, <http://www.charityandsecurity.org/FinAccessPR>

In a report published in 2016, the World Bank Group and ACAMS made a number of recommendations, including the need for greater clarity and consistency about regulatory expectations, greater transparency on how regulators deal with infringements and the harmonization of regulations to facilitate global compliance. The report also suggested that there should be a direct line of communication between the compliance departments of respondent and correspondent banks, and that correspondent banks should be transparent about their reasons for terminating CBRs.⁶

Meanwhile, where the Caribbean is concerned, a discussion paper published in 2016 by Caribbean Development Bank set out a number of possible short-, medium- and long-term goals, which should be targeted by regional stakeholders.⁷ These included recovering lost CBRs and preventing the loss of current CBRs, as well as making CBRs more cost-effective for correspondent banks. The report also highlighted the importance of increasing understanding of the region's AML risk profile and diversifying the range of robust CBR providers to regional institutions.

Increasing transparency

At an individual bank level, local banks are considering which measures they can take to protect their own correspondent banking relationships. While it is impossible to guarantee that a specific relationship will not be terminated, banks can reduce the likelihood of this outcome or increase the likelihood of securing alternative relationships by communicating with correspondent banks in a more transparent way.

By sharing information more effectively, smaller banks can help to reduce their counterparties' due diligence costs, helping to allay concerns about the profitability of specific relationships. Practical measures might include making sure that sufficient

controls are in place, as well as building a gold standard data set which can be used to share consistent information with counterparties.

Experts have also underlined the role that industry utilities for know your customer (KYC) and sanctions screening can play in increasing transparency and sharing information effectively, with central banks leading community initiatives to join utilities in some markets. Shared platforms can act as a repository of relevant data, enabling counterparties to source trusted, up-to-date KYC information and thereby provide greater comfort to correspondents. With a number of different utilities available, it may be prudent for banks to submit their data to several platforms, as long as they can ensure that their data is fully current and that each utility is updated with the same information.


Banks should be aware that taking the necessary steps to distinguish themselves as a trustworthy and compliant banking partner in a higher risk market can actually be a source of competitive advantage. The following recommendations should be considered when banks are seeking to protect their CBRs:

- Work with regional development banks, central banks and industry associations to understand the specific challenges and how best to address these.
- Ensure that you have systems and processes in place to screen transactions, customers and PEPs in line with global compliance standards. Be able to demonstrate that such screening is taking place and being done effectively.
- Join an industry KYC utility. In many cases, the decision whether or not to de-risk is a business one. For example, does the business case for maintaining a relationship justify the cost of performing KYC due diligence and other compliance activities?

By making your information available in a utility, you demonstrate transparency and reduce your counterparty's compliance costs.

- Use data analysis and reporting to demonstrate to your counterparties where your payment flows are coming from and going to (including 'nested' relationships). Be prepared to explain the legitimacy of such flows and answer any questions your correspondent bank might have.
- Talk to your correspondent bank proactively to understand their basis for making de-risking decisions. Agree on an action plan to address any concerns and execute this to demonstrate your commitment to transparency and compliance.

Conclusion

While de-risking can happen for different reasons, it has become apparent that measures originally intended to combat the risk of money laundering and terrorist financing have contributed to the termination of some CBRs. This, in turn, makes it more difficult for payments to be made through legitimate channels—ultimately increasing the risk that illicit transactions will occur. As the industry seeks to overcome these issues, financial inclusion needs to remain front and center, not only because it is essential to society, but also as a means of minimizing illicit flows. 

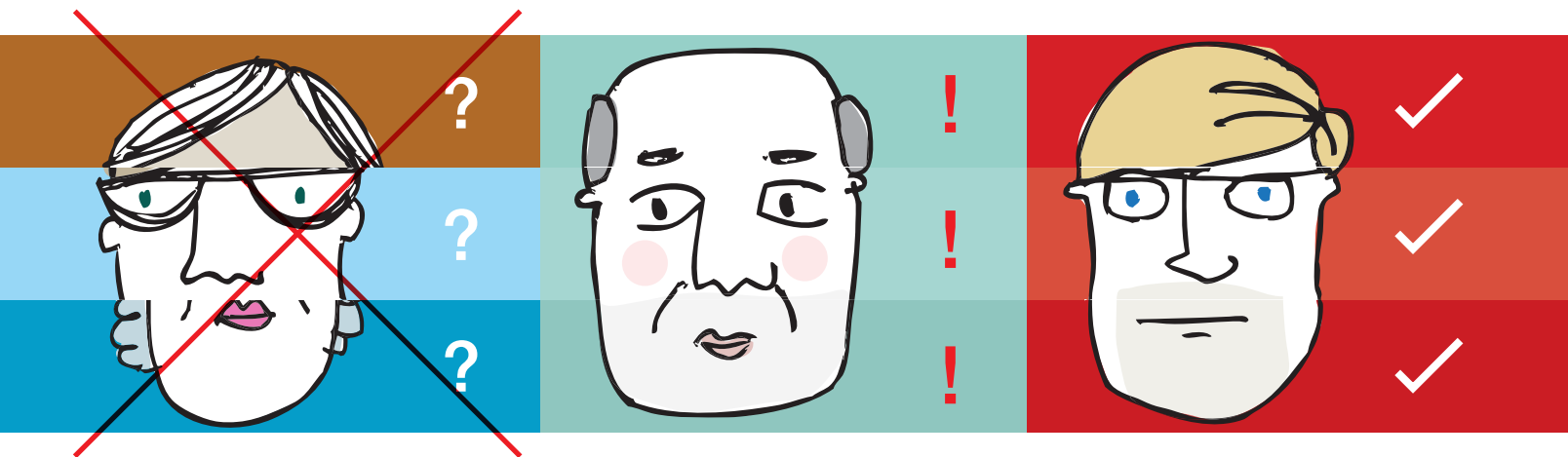
Paul Taylor, head of financial crime compliance initiatives, SWIFT, London, U.K., paul.taylor@swift.com

Juan Martinez, managing director of Latin American and the Caribbean, SWIFT, New York, NY, USA, juan.martinez@swift.com

⁶ "Stakeholder Dialogue on De-Risking—Findings and Recommendations," World Bank Group and ACAMS, 2016, <http://files.acams.org/pdfs/2016/Derisking-Final.pdf>

⁷ Dr. Toussant Boyce, "Strategic Solutions to De-Risking and the Decline of Correspondent Banking Relationships in the Caribbean," Caribbean Development Bank, May 2016, http://www.caribank.org/wp-content/uploads/2016/08/DiscussionPaper_Solutions_De-RiskingCBRs-8-25.pdf

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, maintenance 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 search engine. Hosted and managed by SWIFT, it will enable you to check individual names using a simple, online service built and managed for the industry, by industry experts to world-class standards.

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



20 minute AML investigations

Is there a point of diminishing returns in Bank Secrecy Act/anti-money laundering (BSA/AML) compliance where further investigative efforts within the financial institution's scope is no longer prudent?

Does your institution have what it takes to go beyond establishing a clear suspicious activity and is this a realistic goal within your financial institution's investigative scope?

First, let me never suggest that you should not take prudent steps in regards to satisfying regulatory or compliance demands. What I do want you to consider is, what would be the best, most efficient and effective investigative steps, if they were available to you? From there you can consider the real life limitations and make a decision on the potential productivity in using your available resources. You may just find that your goal and satisfaction may be in reaching an acceptable level of suspicion and uncertainty. The investigative actions available to you may be unnecessarily burdensome and may only highlight the fact that more prudent investigative steps should have been taken.

By no means are investigative resource limitations unique to AML investigators. There are considerably more solvable crimes than ever are solved. The resources available to both criminal and private investigators are inherently too limited and too costly to efficiently or effectively conduct comprehensive investigations into every petty crime and misdemeanor. Community norms and criminal justice experiences will unofficially dictate the level of investigative resources or energy put into investigations. In training new detectives, I have often used the "20 Minute Investigation" concept to help examine the everyday considerations investigators make in resource allocations. This idea may be just as relevant for AML investigators in determining the scope and resources which can or should be put into investigations.

Investigator time

Let us analyze the following scenario. Police are called to a bar for a "domestic disturbance." On arrival, the bartender points to a man and a woman at the bar and tells the responding officers that the man had struck the woman in the face. The woman is weeping slightly and holding a cold beer mug against her cheek. Her cheek is reddened but has no true abrasions. The couple is identified as husband and wife. The husband denies striking her, but separately she tells officers it was all her fault. Officers arrest the husband for domestic assault, take a picture of her face and take down the bartender's information. Although the fruition of the case will take some time, the actual investigation determination took less than "20 minutes."


Now, suppose that it is the same call, but this time the husband had used a beer mug to strike her and this results in a big gash to her face requiring medics, a trip to the emergency room and eventually a number of stitches. This time more formal

CSI type photos are taken, several other patrons are identified as potential witnesses and the mug is collected as evidence. The charge now escalates to a more serious felony. The scene and allocation of resources has appropriately been increased, but the "investigation" conclusion was made in the same 20 minutes.

Again let us take this scenario a step further where the blow to the face by the mug causes the wife's demise. A lot more resources will now be dispatched. Every potential witness is identified, the "crime scene" becomes taped off, and the bar is closed as detectives and CSI are called to investigate. They will closely examine any potential forensic evidence and will be very detailed and deliberate in their actions. Although the process will take considerable time, the investigative conclusion will actually be reached in the same 20 minutes.

We have the same basic investigation in all three scenarios but the severity dictated the investigative resource considerations. Few would argue that applying all the resources used in the last scenario would have been a prudent choice in the first. For AML investigators, the level of potential severity also dictates the allocation and use of investigative resources. The question is: At what point can enough of a conclusion be made to assess if additional resources are needed to support it or not?

For AML investigations the severity is more often measured in dollars than in blood, but the principles are the same. Various crimes have various manifestations as to what may be observed or identified during the financial activities associated with them. However, these financial manifestations are rarely unique to a specific crime and will share traits within the general



criminal spectrum. That can be a very diverse spectrum. A conclusion confirming suspicious activity might be made in 20 minutes but the underlying specific criminal activity may require considerably more resources. Some of those resources may not be within the financial institution's scope. Time and time again AML professionals will seek training and guidance for identifiers associated with a specific criminal activity. Could it be drug dealing? Human trafficking? Terrorist financing? Certainty is the desired goal, but is it a realistic one?

Take two pills

Take the case of two doctors who both came to the attention of the BSA/AML departments at their respective financial institutions when a seeming sudden influx of potentially structured cash deposits were identified. After the discovery of the cash anomaly, what is the next best course of investigative action? To either confirm or dispel the reason of the suspicious activities? Let us look at the conclusions eventually reached in these cases and analyze if it could have been accomplished efficiently through other investigative steps.

In one case the doctor had become frustrated with insurance hassles and decided to go rogue. He quickly devolved into a cash-only practice primarily catering to prescription opiate drug abusers as his patients. A steady stream of disheveled and often disorderly patients (typical of addicts in need of a fix) was a common sight around his office. Neighboring businesses also began to take notice. There was even an uptick in petty crime around the area. Each day the doctor would collect and deposit up to \$8,000 in cash from office visits which took little more than the time that he needed to write out a prescription form. It was no surprise to anyone familiar with the doctor when a couple of his patients robbed him on his way to the bank. That robbery actually became the catalyst to a more serious investigation into the doctor's activities. The doctor, eventually confronted with both drug and financial violations, entered a plea agreement with prosecutors.

Another doctor had started making regular and fairly obvious structured cash deposits. In his case, it turned out that he found a niche market primarily with an immigrant community where "off the books" employees lacking insurance were common. For a reasonable price, in cash, he offered access to a physician and basic medical care. On the positive side, his patient base would otherwise be crowding emergency rooms for routine medical issues. Word of mouth kept him overflowed with both patients and cash as well. His efforts in trying to keep his cash influx off the books, as well as away from the tax man, would lead him to eventually enter a guilty plea for BSA-related violations.

After the cash anomalies were identified the next investigative steps taken by investigators in both cases was doing an actual site visit. In both cases a probable conclusion of what was taking place was apparent after as little as "20 minutes" worth of observations. For the first doctor, the investigators readily observed these questionable "patients" loitering in and around the office displaying all the characteristics of addicts needing a fix. The conclusion was made quickly.

However, the action plan to abate this nuisance would require multiple enforcement agencies and departments coordinating their efforts.

For the second doctor, investigators would observe that there was nearly always a full lobby of immigrant workers and their families, including crying babies, from opening to closing. On your average Friday the doctor could also be observed walking to his bank (about a block away) and back multiple times.

By doing the same extensive and time consuming detailed analysis of either doctor's transactional data, you might also reach similar conclusions. With the "pill doctor" you would have noticed a lack of invoices or purchases for medical supplies commonly used in an active doctor's practice. There was also a distinctive lack of insurance company debits or credits as well as no checks, credit or debit card activity for the ever more common copays these days. This would certainly not be indicative of a traditional medical office practice. That would add to "suspicious activity" but not to an investigative conclusion. The financial activities need context to move beyond suspicious. That context in this, and most AML cases, will be outside the financial activities. The financial institution activity is only a part of the totality.

For the "immigrant doctor" there was lots of cotton balls, tongue depressors and sundry medical supplies needed to treat a plethora of ailments and wounds. Those expenses and invoice payments were apparent, but are also "normal" for any primary care physician. There was still a lack of insurance, credit card, or even check payment activities. That might indicate a cash centric business practice but not why a physician would choose this route. You also do not have enough information to conclude you know all the accounts the doctor may have. Although detailed

FINANCIAL ACTIVITIES NEED CONTEXT TO MOVE BEYOND SUSPICIOUS

deposit and check analysis may find other potential account relationships you still would lack certainty.

Worth the time?

From an AML perspective were these site visits the most efficient and prudent investigative actions in these cases after identifying the cash anomalies? What others might come to mind?

If your AML investigation resources do not allow for such field work, you might start chasing current hot AML topics such as human trafficking, drug dealing or terrorist financing, hoping your identified indicators can be tailored to fit one of these violations. That is unless you are already familiar or aware of the seemingly endless possibilities that can make up money laundering schemes with these same indicators. These possibilities can include regional issues with very lucrative schemes that involve commodities or items related to regional circumstances. Tax and regulatory issues have made many otherwise innocuous commodities subject to lucrative black and gray markets with corresponding BSA/AML issues. In many of these cases the amounts and quantities involved often exceed their more purely contraband counterparts, like drugs.

Currently, wheels of cheese are being smuggled from the U.S. into Canada in amounts of both dollars and products that rival many drug cartels. Heavy taxes and regulation on dairy products in Canada have caused many pizza restaurants in Canada to find a cheese "source" across the border. Although pizza shops have had some notoriety in the past as being used as fronts for money laundering, would an AML investigator equate the cash anomalies at a cheese-related business with this activity? How about a Canadian pizza shop with "cash out" anomalies? Did those previous investigators ever have to consider that part of the scheme was actually ending up as part of the toppings. I do not recall felonious cheese schemes as being an AML hot topic!

Virginia and Missouri have some of the lowest tobacco taxes and regulations in the nation. The smuggling of these cheaper cigarettes has created black and gray markets in regional states with higher taxes. These schemes are


often easier, more lucrative, and usually far less risky than finding a connection to the illicit narcotics counterparts. Big box wholesale clubs are more reliable and safer suppliers than back alley pushers in obtaining a quantity of cigarettes for profitable re-sale a state or two away.

Do other financial indicators ever eliminate a potential drug dealing or other nefarious nexus? AML training has often included how convenience stores are used in all manners of money laundering schemes. Should it include the possibility that the source of the illicit funds might be sold in plain sight?

Poaching and ivory smuggling has also received considerable international attention lately and only now is the analyzation of potentially associated financial activity behavior being considered in the identification, interdiction and abatement planning. Will this prompt a search for new AML alert indicators or actually result in a second look as reasons for already existing ones?

Although criminal activity may have identifiers associated with it, the accompanying activities at financial institutions may be similar or the same for a wide variety of violations. What needs to be added is context. What further can be observed or identified in those financial activities toward that specificity will likely be innocuous nuances requiring endless examination and the crunching of numbers. In most cases, this micro transactional analysis is a very inefficient means of trying to make an investigative determination, which can more effectively and efficiently be made through leads or evidence outside of a financial institution's scope.

How many nuances to identifying specific violations should your AML training cover?

Are you certain? 

*Steve Gurdak, CAMS, supervisor,
Washington Baltimore HIDTA,
Northern Virginia Financial Initiative
(NVEI), Annandale, VA, USA,
sgurdak@wb.hidta.org*

ACAMS® | Certificates

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



Sanctions Compliance

Learn the crucial sanctions compliance principles all compliance staff should understand. The learnings gained from this course fit into any current sanctions compliance program, helping to improve your controls.



KYC CDD

Learn to assess what you need to know, explore where to find the answers, organize your customer information in a meaningful way, and present your findings and Customer Due Diligence requirements clearly to all stakeholders.



Counter-Terrorist Financing (CTF)

Your team will get a clear understanding of how terrorism works and how it is financed, how to identify possible threats to your institution, how to mitigate terrorist financing risk, and how to build a Rapid Response Team.



AML Foundations

AML Foundations is a stepping stone for entry-level employees not yet ready for CAMS certification and for business line staff who need solid AML training now so they can add more value on the job today.

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

Register to earn your training certificate

acams.org/certificates



DEVELOPING TERRORIST FINANCING TYPOLOGIES FOR AML PROGRAMS

Developing terrorist financing typologies for anti-money laundering (AML) programs requires understanding. You must understand the terrorist threat environment, emerging terrorist trends, the funding flows terrorists rely on to sustain their operations and your institutional risk for being used to facilitate terrorist funding flows. When you understand these dimensions and place them in context with each other, you should be positioned to develop viable terrorist financing typologies. This can be a daunting challenge because there are no silver bullets or smoking guns. In addition, the challenge of identifying terrorist financing is exacerbated by the breadth of the terrorist landscape in terms of funding sources, funding streams and use of funds.

It is possible to identify terrorist financing preemptively, but the likelihood is not probable until after a terrorist event takes place. We normally identify terrorist financing reactively, after the fact, through negative news. Our challenge is to improve the likelihood and thereby increase the probability of identifying suspicious activity before that activity evolves into a terrorist event. Increasing the probability of identifying terrorist financing begins with building a foundation through understanding the following four dimensions: the threat environment, emerging trends, funding flows and institutional risk. By assessing each element and placing them in context with each other in a matrix or analytical report or assessment, you can take more generic risk indicators or red flags and make them more specific to your institutional risk. There are numerous reference guides listing terrorist financing red flags and typologies on a broad or generic level. Taking those broad typologies and assessing them against your institution's risks will lead to developing more focused and institution-specific red flags and risk vulnerabilities.

In the U.S., a good example for red flag guidance is contained in the Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/AML Examination Manual. Appendix F of the FFIEC Examination Manual lists money laundering and terrorist financing red flags. The terrorist financing red flags are listed on page F-9. On a regional and global level, the Financial Action Task Force (FATF) has published numerous terrorist financing typologies reports that offer meaningful guidance for identifying terrorist financing. In addition, national financial intelligence units, such as the Financial Crimes Enforcement Network (FinCEN) in the U.S. and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) provide valuable information regarding terrorist financing. Another excellent source for building terrorist financing typologies is from law enforcement charging documents, such as criminal information, indictments, arrest and search warrants, and plea agreements. These charging documents usually contain an affidavit with a statement of facts, which sets forth the scheme or scenario used, to include money laundering. In

addition to these sources, numerous publically accessible online websites, think tanks, private intelligence services (some being subscription services), and other government or private sector sources, provide research guidance.

In developing your institution-specific terrorist financing typologies, it is important to be forward thinking, adaptable, attentive and innovative. You must be forward thinking and adaptable regarding the threat environment and emerging trends. You must be attentive to visualizing funding flows and minimizing false positives. You must be innovative in developing your monitoring and analytical capabilities to mitigate your institutional risk.



As a somber reminder, there is no easy answer or monitoring tool to readily identify terrorist financing. It takes commitment, understanding and visualization. First, you have to make a commitment to build adequate capacity. Second, you must understand the problems and challenges. Third, you must visualize the flow of funds from the point of origin to the point of distribution or intended distribution.

The following is an outline of the threat environment, emerging trends, funding flows and risk from an AML compliance perspective. One consideration that stands out from the outline is the myriad of variations terrorist financing can take. That is one reason why it is imperative to place these dimensions in context with each other and develop terrorist financing typologies specific to your financial institution. Identifying all-encompassing warning signs is highly improbable. However, taking a

more measured and reasonable approach to identifying red flags and risk factors that are more specific to your financial institution makes it more possible to identify terrorist financing.

Terrorist threat environment

From the government perspective of law enforcement, intelligence agencies, sanctioning bodies, diplomatic services and the military, the threat environment is primarily a national security concern. A major factor is the level of geographic and physical threat. From a financial institution perspective the threat environment is primarily driven by economic risk.

Both the national security and economic threat environments begin with terrorist actors. We must focus on both organizations and individuals aligned with organizations—either as organizational members or as aspirants—who are inspired by the group and in many cases, pledging their allegiance. This is where the broad expanse of the terrorist landscape begins. In today's world the biggest terrorist threat to most countries is posed by Islamic terrorists. By no means are those jihadists (those who use a false sense of Islam to front their ideology) the only terrorist threat we face. There are many terrorist threats. However, the most acute is the threat of Islamic terrorism.

From a financial institution standpoint, who are we dealing with? Who are our customers? From an organizational perspective, we should look at terrorist groups as corporations and assess their business models. Like financial institutions, terrorist organizations may share many similarities. However, each group deals with different circumstances, which make them unique from one another. Based on their business model, they each have distinct funding requirements. For example, if you compare and contrast organizations such as the Islamic State, al-Qaeda and Hezbollah from a business model perspective, you can begin to assess their similar and differing funding requirements. In building a business model for a terrorist organization you should assess the following five components needed to establish and sustain their operations:

1. What is their mission statement? What does the organization aspire to be?
2. What is the desired infrastructure required to support the mission statement?
3. What are the funding requirements needed to support the desired infrastructure?
4. What are the funding sources needed to meet the funding requirements?
5. What are the funding mechanisms (formal and informal banking channels) needed to support the flow of funds through the process of raising, storing, moving and spending money?

In addition to dealing with organizations, financial institutions must be prepared to deal with the individual terrorist actors affiliated with terrorist organizations. The roles of individuals include those of leaders, facilitators, fundraisers, recruiters, foot soldiers or operatives and individuals influenced by and aspiring to support a terrorist organization. Like the organizations themselves, each role or position has specific funding requirements. Some funding characteristics for each role will be similar and some unique to each position and the individual needs of the terrorist actor. At least one commonality they would all likely share is the need to use the formal and informal financial systems to access and spend money. Financial institutions must assess the likelihood of dealing with individual terrorist actors in the roles previously mentioned and in what capacity that would be.

In most instances, when developing red flags or typologies for terrorist actors, financial institutions are inclined to use more generic red flags and not focus more granularly on warning signs for the different specific roles and responsibilities individual terrorist actors perform. Through case studies, law enforcement contacts, analysis of internal financial intelligence and external information sources, such as FATF terrorist financing typologies focused on individuals such as foreign fighters, financial institutions should develop customer profiles for each individual terrorist actor position. In addition,

financial institutions should assess the likelihood of dealing with individuals in each possible role.

Emerging terrorist trends

Terrorist trends are driven by inherent and adaptive factors. Inherent factors include ideology and politics. They tend to be more static and predictable. The combination of ideology and the aspiration of a terrorist organization, coupled with the political environment in a country or region in terms of the political capacity, corruption and lack of governance, affords terrorist organizations opportunity and a safe haven for growth. Terrorist organizations leverage such opportunity with their adaptability. Adaptive factors include technology and counter-terrorist tactics. They are non-static and tend to continuously evolve. Terrorist organizations exploit and adapt to technology for propaganda, recruitment, fundraising and more. They also

al-Nusra Front, the al-Qaeda affiliate in Syria, also benefited from the influx of foreign fighters to the region. In the latter part of 2016 and into 2017, as the international focus against the Islamic State caused them to lose considerable territory and jeopardize their caliphate, the Islamic State called for recruits to stay home and commit terrorist acts in their home countries. As a result, the threat of homegrown violent extremists and returning foreign fighters has continued to evolve as a significant dangerous trend.

The recent emergence of homegrown violent extremists has led to the phenomenon of the leaderless terrorist model. Instead of a command and control structure, where terrorist attacks are directed by the organization, the group (in this case the Islamic State) encourages homegrown violent extremists to commit a terrorist attack, where the opportunity presents itself, at the attacker's discretion.

THE RECENT EMERGENCE OF HOMEGROWN VIOLENT EXTREMISTS HAS LED TO THE PHENOMENON OF THE LEADERLESS TERRORIST MODEL

adapt to counterterrorism measures taken by the public and private sectors in order to avoid detection and to sustain their operations.

In the last few years, we have experienced the emergence of the Islamic State as the primary terrorist threat to Western nations. Their ability to establish a caliphate in large portions of Iraq and Syria, due to poor governance, allowed the Islamic State to gain strength and incredible wealth. Consequently, they were able to attract thousands of foreign fighters. While the caliphate was strong in 2015 and for the first half of 2016, the emerging and current trend was travel of radicalized jihadists to join the Islamic State as foreign fighters in the caliphate. The Islamic State also encouraged radicalized individuals, who could not travel, to commit terrorist acts at home. The

Funding flows terrorists rely on

There are primarily three funding flows or funding streams terrorists rely on; however, there are many variations to the three funding flows that terrorists can follow. The key for them is having consistent access to funds at select intervals between the point of origin and the point of distribution.

The first funding flow is from the point of origin or source of funds to the organization. Amounts will range from small donations below \$100 to revenue streams in the millions of dollars from business holdings, criminal activities, wealthy donors, state sponsors and other sources. This funding stream requires considerable bandwidth to move money.

The second funding flow is from the organization to support an operation. Amounts will generally run between \$1,000, or lesser amounts, to multiple thousands of dollars. The money could be sent directly from a group leader or financier to a single jihadist or group of jihadists working together. The more likely scenario for money flowing from the organization to support an operation is to send it through a facilitator to the operative or group of operatives acting in concert. In this scenario, the thousands of dollars flowing from the organization to the facilitator will be further broken down by the facilitator into smaller increments to be forwarded on to the operatives. This would be a form of microstructuring, which could be extremely difficult to detect.

The third funding stream is the funding from the operation to the operatives. This funding stream ranges from hundreds to the low thousands of dollars, as previously described in the step between the facilitator and the operatives. The funding to the operatives would likely be spent in low increments to pay for a terrorist activity. This would represent the final disposition of funds.

The third funding stream, funding to the operatives, has taken on a new variation in the form of a reverse flow. Instead of the money flowing down from the organization, the money is being generated directly by the operatives through their employment income, government assistance, proceeds of criminal activity, family donations and other sources. Essentially, the operatives—mostly acting as aspiring foreign fighters or homegrown violent extremists—are responsible for the source of funds themselves, as opposed to the terrorist organization raising the money for them.

Coupling the differing types of terrorist actors with the multiple variations of the three primary funding streams, the magnitude of the terrorist landscape can become unwieldy and overwhelming.

Institutional risk

With the overwhelming bandwidth involving terrorism, it is virtually impossible to develop and implement monitoring systems to identify the full gamut of terrorist financing. This is why

identifying and assessing specific institutional risk is critically important. All financial institutions regardless of their size, location, products, services or business lines are vulnerable to terrorist exploitation. They are vulnerable to facilitating the funding needs of terrorist actors to include organizations and individuals.

The risks of being exploited by terrorist organizations will differ from the risk of dealing with terrorist operatives. In assessing your institutional risk for terrorist financing, you should evaluate your risks to measure both the likelihood of facilitating terrorist organizational activity and individual operative activity distinctly from each other. You must understand and visualize who you are dealing with and in what capacity. You should develop red flags and typologies that you are more likely to encounter within your institution. The risk categories you should review include geographies, customers, products, services, funding flow and distribution channels.

For terrorist organizations, you should determine which designated organizations pose a current terrorist threat. Based on the above risk categories, you should assess and rank the likelihood of your institution dealing with the different terrorist groups. You should assess the potential customer risk by developing a business model for the terrorist organization and assessing funding flows and distribution channels for potential touch points with your institution.

For individual operatives, you should develop potential scenarios for each of the roles a terrorist might engage in, including the responsibility of leader, facilitator, fundraiser, recruiter, foot soldier or operative, and an individual influenced by and aspiring to support a terrorist organization. Based on the risk categories, you should assess the likelihood that your institution would deal with individuals that fit these roles and responsibilities.

In light of the threat posed by foreign fighters and homegrown violent extremists, you should pay particular attention to the threats posed by individuals influenced and aspiring to support terrorist organizations. The FBI website possesses many case studies for foreign fighters and violent

homegrown extremists. Another good source for individual case studies is the Investigative Project on Terrorism.

Placing the terrorist landscape in an AML context

Depending on the size of your financial institution, you should build a dedicated team or designate one or more individuals to assess your specific institutional risk for facilitating terrorist financing. Financial institutions should consider building financial SWAT teams or Critical Incident Response teams, analogous to the law enforcement SWAT team concept, to deal with select AML challenges, such as terrorist financing. Regardless of resource constraints, financial institutions should dedicate resources to develop terrorist financing typologies and to respond to terrorist incidents or suspicious activity that could potentially identify terrorist financing.

Your Critical Incident Response team or designated terrorist financing resource should look at terrorism from an AML perspective and place the terrorist landscape in an AML context. This requires linking the threat, emerging trends, funding flows and risk together in a matrix, analytical report or terrorist financing assessment that can serve as the framework for building terrorist financing typologies specific to your institution.

For example, for the purpose of this article, a sampling from each of the four dimensions will be placed in context with each other to use as a framework to build institution-specific terrorist financing typologies. Please note that these are not all encompassing examples.

Beginning with the terrorist threat environment, groups of significant concern include the Islamic State, al-Qaeda, al-Qaeda affiliates including the al-Nusra Front and al-Qaeda in the Arabian Peninsula (Yemen), the Taliban (Afghanistan), al-Shaabab, Boko Haram and Hezbollah. The Islamic State has branched out from Iraq and Syria to other parts of the world. They pose a significant threat to the U.S., Europe and many other countries. Although their caliphate may soon be destroyed, they will continue to

operate as an insurgency and remain a serious threat. Al-Qaeda has quietly reconstituted itself and poses a significant threat. The Taliban in Afghanistan has gained control of more territory. In addition to raising funds by controlling drug trafficking, they are now raising considerable funds through taxation and extortion in the territory they control. Al-Shaabab operates from Somalia and continues to pose a regional and to a lesser degree global threat. Boko Haram operates in Nigeria and neighboring countries. They have pledged allegiance to the Islamic State and pose a regional threat. Hezbollah is the most dangerous terrorist organization in the world. They are primarily supporting Syria at this time. If they feel threatened by the West, they will pose a threat. Hezbollah is also the best organized crime family in the world. They possess a global infrastructure that supports their terrorist activities and their criminal enterprise.

From the standpoint of emerging terrorist trends, foreign fighters and homegrown violent extremists radicalized and recruited by the Islamic State, and to a lesser degree al-Qaeda, continue to be the major trend of concern. The Islamic State will likely lose its caliphate in Iraq and Syria within the next year. They will evolve into an insurgency group and will continue to strike out against the West through homegrown violent extremists and returning foreign fighters. They will use a leaderless terrorist model and encourage their followers to attack at their individual discretion. Al-Qaeda has quietly reconstituted itself and the core group will reemerge as a formidable threat. As they gain and hold more territory in Afghanistan, the Taliban will increase their wealth and consequently their strength and pose a greater threat to the shaky stability in Afghanistan.

When considering the funding flows terrorist actors rely on, we need to assess them at both the organizational and individual levels. This requires following the flow of funds through the three funding streams (organizational, operational and individual), and variations thereof. Terrorist actors must have consistent sources of funds and access to funds on an ongoing basis in order to sustain their organizations and operations. For each of the most

significant terrorist groups identified that pose potential institutional risk of facilitation at the organizational and/or individual operative level, you should assess the three funding streams and the variations thereof, and visualize how they could flow through your institution.




The final analytical step is to assess your specific institutional risk against the threat, trends and funding flows. How are you affected by geographic risk domestically, regionally and/or globally? What steps can you take to know your customer risk and to assess which customers could be terrorists or terrorist supporters? This is where (from a terrorist group standpoint) you should assess the business model for the most significant terrorist groups. On an individual level, how do you know which customers could be terrorist actors in the role of leaders, facilitators, financiers, recruiters, foot soldiers or operatives, or aspirants, inspired by the Islamic State or other groups? This is where you need to build individual typologies for each role individual terrorist actors might engage in. These typologies can be built from red flags, such as from the FFIEC Manual, FATF guidance and case studies from sources like the FBI and Investigative Project. You should also assess the risk for products, services and business lines. In addition, when assessing these risk categories, you should consider and visualize your institutional risk for facilitating funding flows and distribution channels.

Conclusion

As evidenced in consideration of the scope of the threat environment, emerging trends, funding flows and institutional risk, we face a daunting task when it comes to identifying terrorist financing. There are no quick fixes or shortcuts from a financial institution standpoint. What is required is a meticulous, focused and forward

thinking approach. We must methodically take generic and broad based red flags and warning signs and meticulously shape them into institution-specific risk indicators.

This requires understanding and commitment. We must understand the problem or threat and we must dedicate adequate resources to address the problem. To best meet this challenge, we must place the threat environment, emerging trends, financial flows and institutional risks into context with each other. Once the full context is assessed and placed in perspective and focus, we can more effectively and efficiently respond to the challenge. This will allow us to go from a reactive posture to developing proactive strategies.

Finally, in order to maximize the benefit of meaningful financial intelligence we must be forward thinking and innovative about exploiting the information. How can we most effectively improve efficiencies to develop timely and actionable financial intelligence? As an example, one of the biggest challenges we confront today is identifying homegrown violent extremists and foreign fighters. Most homegrown violent extremists have jobs and their customer profiles do not raise any suspicions until they are reported in negative media for committing or attempting to commit a terrorist act. Likewise, foreign fighters who successfully travel to Syria are gone before warning signs are detected. One way to deal more proactively with these challenges is to conduct a cluster analysis or behavioral analysis model whereby you group a set of objects in such a way that objects in the same group are more similar to each other. In addition to your base line transaction monitoring, another example of innovation is to take specific typologies and develop rules for targeted monitoring, where you are monitoring for more specific activity. These examples demonstrate that the more proactive and innovative we can be, the more possible and probable we can make it to identify terrorist financing. 

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



THE SECRET FORMULA REVEALED!

Countless variables exist when it comes to managing compliance in a global economy, especially as you work across disparate compliance systems. Your business faces enormous challenges in solving this equation—and stiff penalties for one small misstep. With CSI, you get a **technology partner that can deliver a collaborative platform** that connects existing systems, creating a centralized compliance system of record. Our WatchDOG® Elite solution provides the secret formula you've been waiting for.



csiweb.com/Secret

Enterprise Risk Management • WatchDOG® Watch List Screening • Compliance Software & Services • Cyber & Information Security Services

ACAMS® | Affiliate Member *Gold*

CELEBRATING 15 YEARS OF ACAMS TODAY



Fifteen years ago, the *ACAMS Today* newsletter—now a magazine—launched with a mission to become the premier publication for the career-minded financial crime detection and prevention professional.

Years later, the *ACAMS Today* magazine gained popularity in the financial crime prevention industry as the go-to magazine for AML/financial crime prevention professionals. The magazine continues its mission as a dedicated source for insightful and timely AML/CTF-related content.

The magazine has won a significant amount of awards in both content and design, and remains the leading publication for career-minded professionals in the financial crime detection and prevention field. This section celebrates 15 years with interviews on the evolution of *ACAMS Today* and the growth of ACAMS, an infographic revealing interesting facts on your award-winning magazine, a retrospective on our cartoons and a new section titled “AML Classics” showcasing articles from past editions.



JOHN J. BYRNE, CAMS: 15 YEARS OF ACAMS TODAY

A *CAMS Today* sat down with ACAMS Executive Vice President, John J. Byrne, Esq., CAMS, to discuss the last 15 years of the *ACAMS Today* magazine's progression and to reminisce over how the anti-money laundering (AML) environment has changed.

Under Byrne's tutelage, the Association of Certified Anti-Money Laundering Specialists (ACAMS) has grown to almost 45,000 members and has evolved into a global organization that develops AML/sanctions/financial crime detection programs and certifies specialists in financial and non-financial businesses and government agencies.

Byrne is an internationally known regulatory and legislative attorney and one of the leading AML voices for 30 years. He has experience in a vast array of financial service related issues, with particular expertise in regulatory oversight, policy and governance, AML, privacy and terrorist financing. He has written over 100 articles on AML, asset forfeiture and privacy; represented the banking industry in this area before the U.S. Congress, state legislatures and international bodies such as the Financial Action Task Force (FATF); and appeared on *CNN*, *Good Morning America*, the *Today Show* and many other media outlets.

Byrne has received a number of awards, including the *Director's Medal for Exceptional Service* from the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the ABA's *Distinguished Service Award* for his career work in the compliance field.

Byrne is a graduate of Marquette University in Milwaukee, Wisconsin (1978) and the George Mason University School of Law in Arlington, Virginia (1983). Byrne's blog, "AML, Fraud and Other Things," can be found on www.bankingexchange.com as well as on the ACAMS website. He also hosts the *AML Now* podcast and you can follow him on Twitter @jbacams2011.

ACAMS Today: Which ACAMS Today article has been your all-time favorite?

John Byrne: For me it is more about my favorite themes and that is clearly the Law Enforcement Edition we now produce. The AML community can only succeed when we recognize the importance of partnerships. Partnering in AML depends so much on law enforcement and to be able to recognize their work, the issues they find important and what strategies they believe are needed to combat money laundering and financial crime.

AT: How has the ACAMS Today magazine evolved during the last 15 years?

JB: The biggest change is the expansion of AML to now include gaming, Fintech, real estate and other aspects outside of traditional banking and our coverage of those changes.

AT: Since becoming ACAMS executive vice president, you have been a constant contributor to the ACAMS Today magazine. What is the inspiration behind your column?

JB: I try to both focus on a few articles in that edition and call out some members who have performed important work for the community. Sadly, I have also had to note the passing of a number of AML leaders.

AT: What hot topic do you see dominating the financial crime field in 2017?

JB: The most important issue is a global problem that touches AML—de-risking and financial access. While admittedly not solely a compliance focus, the lack of clarity from regulators or from policy interpretation coupled with financial institutions having to

make risk and business decisions have all caused economic heartache for a vast array of entities. There can be no greater topic for AML and financial professionals and one where we can create a solution.

AT: You were featured on the cover of one of the AT magazines, do you remember which edition and do you remember the size of the membership at that time?

JB: Dan Soto and I were featured when I took over as the ACAMS Advisory Board Chair back in January 2007. At that time, our membership was around 5,000 and as we know, we have been fortunate to grow to almost 45,000 in 2017. The growth can clearly be attributed to the vast expansion of AML professionals throughout the globe and the career benefit of our CAMS designation for both the private and public sectors. Fortunately, Dan and the entire advisory board gave us direction and assistance on how to stay relevant to the ever-growing community that AML has become.

AT: Your AML blog always has a music theme, how has music influenced your writing style?

JB: Not sure that music influences how I write, but what has always interested me is when a song has good lyrics. My generation was fortunate to have musicians who agreed with that and I do try to match a song with a blog theme. Sometimes it is a stretch, but it forces me to do some musical research, which is something I thoroughly enjoy. 🎵

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

ACAMS[®]TODAY

5th ANNIVERSARY EDITION

The Anti-Money Laundering Association for the Career-minded Professional

ACAMS membership
reaches 5,000! p.6

Changing of the Guard

- John J. Byrne, CAMS takes
over as ACAMS Chair from five-
year veteran Dan Soto, CAMS

JANUARY/
FEBRUARY 2007
VOL. 6 NO. 1

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

www.ACAMS.org

www.ACAMS.org/espanol



DAN SOTO, CAMS: ACAMS' 15 YEARS OF GROWTH

A *CAMS Today* caught up with Dan Soto, chief compliance officer for Ally Financial, Inc., where he is responsible for its enterprise-wide compliance activities, to discuss the last 15 years of ACAMS' growth.

Before joining Ally, Soto spent two years with Wachovia/Wells Fargo in anti-money laundering (AML) and retail banking compliance; was the chief compliance officer for Royal Bank of Canada-Centura for three years; and spent eight years with Bank of America in the global AML compliance function.

Prior to joining the private industry, Soto was in the public sector as a commissioned bank examiner where he spent six years with the FDIC and nearly 10 years with the Federal Reserve Board.

Soto is based in Charlotte, North Carolina and he is a faculty member of the American Bankers Association's National Compliance School and an advisory board member of the Association of Certified Anti-Money Laundering Specialists (ACAMS) and the BSA Coalition.

ACAMS Today: How has ACAMS changed in the last 15 years?

Dan Soto: Although ACAMS has always strived to be an expansive forum, both in terms of geographical reach and membership, I had no idea just how powerful the ACAMS brand would become. We now have membership all over the world, but just as importantly, we have expanded in membership, specialty certifications and chapters are constantly being added.

AT: How has the role of the compliance officer evolved in the last decade?

DS: The role of the compliance officer has evolved from one that operated behind the scenes in establishing a compliance program to one that is now front and center in not only setting a sound compliance program, but communicating with various stakeholders (e.g., boards, executive management, regulators, etc.).

AT: Which ACAMS Today edition or article has been your favorite?

DS: My favorite article is "Training Your Employees," by Kevin Anderson, who is with Bank of America. When I left the government in 1998 to join NationsBank, Kevin and I had a two-person shop operating out of D.C., supporting wealth management/private banking AML compliance programs. Kevin is and remains one of the most knowledgeable people I know and I was proud to see his first article published by ACAMS in January/February 2007.

AT: As an ACAMS advisory board member, can you share a sneak peek of the important issues discussed during your board meetings?

DS: Boards are passionately interested in whether AML programs are working as intended, that staff is appropriately educated (and certified), and that the board members receive timely, accurate and easily understood reporting as to the "health" of the programs.

AT: What is the next big theme we should be discussing in the fight against financial crime?

DS: The theme constantly heard these days has moved from the convergence of AML and fraud programs to the convergence of AML/fraud and cybersecurity. The ability to leverage resources across these three areas is daunting.

WE NOW HAVE MEMBERSHIP ALL OVER THE WORLD


AT: You were featured on the cover of one of the ACAMS Today magazines, do you remember which edition and do you remember the size of the membership at that time?

DS: Unfortunately, I don't, but I am guessing it was one of the early editions (perhaps even the first) and the membership was likely fewer than a thousand.

AT: You are right, it was one of the earlier editions, but the membership had reached 5,000. You were on the cover of the January/February 2007 edition.

DS: Interesting that the same edition in which I was on the cover is the same one where Kevin Anderson wrote his first article.

AT: Besides the ACAMS Today magazine, what other AML or financial crime prevention resources have helped you in your day-to-day compliance work?

DS: There are numerous AML-related publications. I personally use ACAMS' moneylaundry.com to keep up-to-date with world events. 

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

KARLA MONTERROSA-YANCEY, CAMS: 10 YEARS OF AN EVOLVING ACAMS TODAY



For the love of the game

This edition's headline articles combine two of my greatest loves: Soccer (or as the rest of the world knows it: football) and art. Why do I love soccer? I grew up with soccer in my home. My family looked forward to watching the World Cup every four years. We rooted for our favorite teams and my father and I would take the time to analyze the beautiful game. We would study the formations of each team, discuss if the team had more of an offensive or defensive style of play, and wonder why the coach was using certain players and not others. As we watched, we would wait for one of those special moments that soccer is known for: an offensive player dancing with the ball and beating the defensive player, the perfectly timed pass, the well taken goal and then the exultant cry of the enthusiastic announcer exclaiming, "GOOOOOOOOOOOOOOOOOOOOOOAAAL!"

So entrenched was soccer in my home that every one of my siblings played soccer and I even had the opportunity to be an assistant coach for a high school team. There are many people out there that can relate to the deep love and tradition that the beautiful game has brought to their lives. Camaraderies are built by jointly cheering for one's nation, adopted nation or simply another nation just because they play the game beautifully. However, the beautiful game has been tarnished by the corruption allegations leveled against its governing body FIFA. In the lead article, *The World Cup of fraud*, author Dennis Lorniel eloquently describes the serious misconduct that led to the

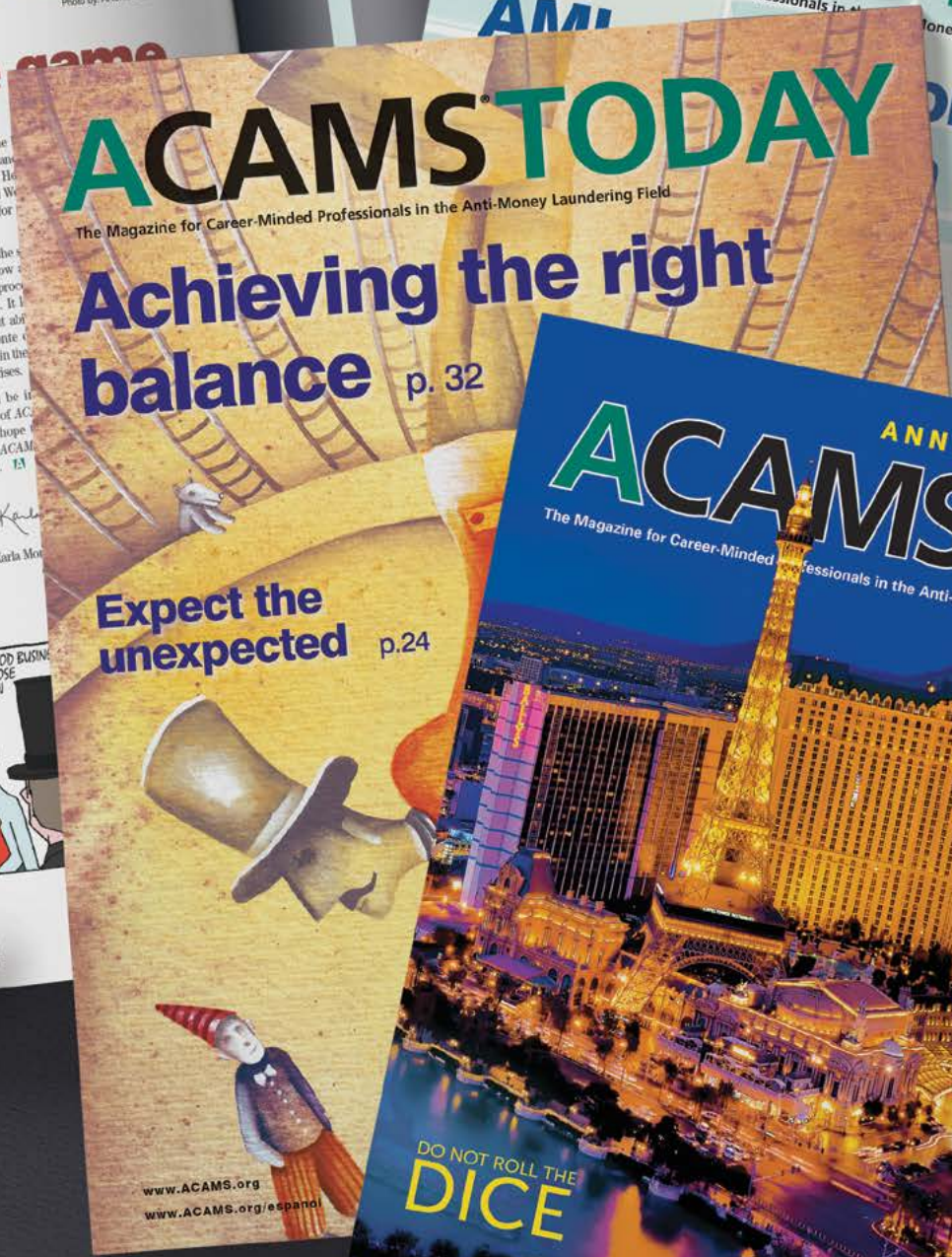
charges against FIFA by the Revenue Service, Richard W. Fiermonte describes how launder and hide illicit proceeds and inspires the mind. In the article, Fiermonte co-opted by criminals in the of their illegal enterprises.

I hope you will all be in the Conference edition of ACAMSTODAY working on it. We hope to see you at the September for the ACAMSTODAY Crime Conference. **TY**

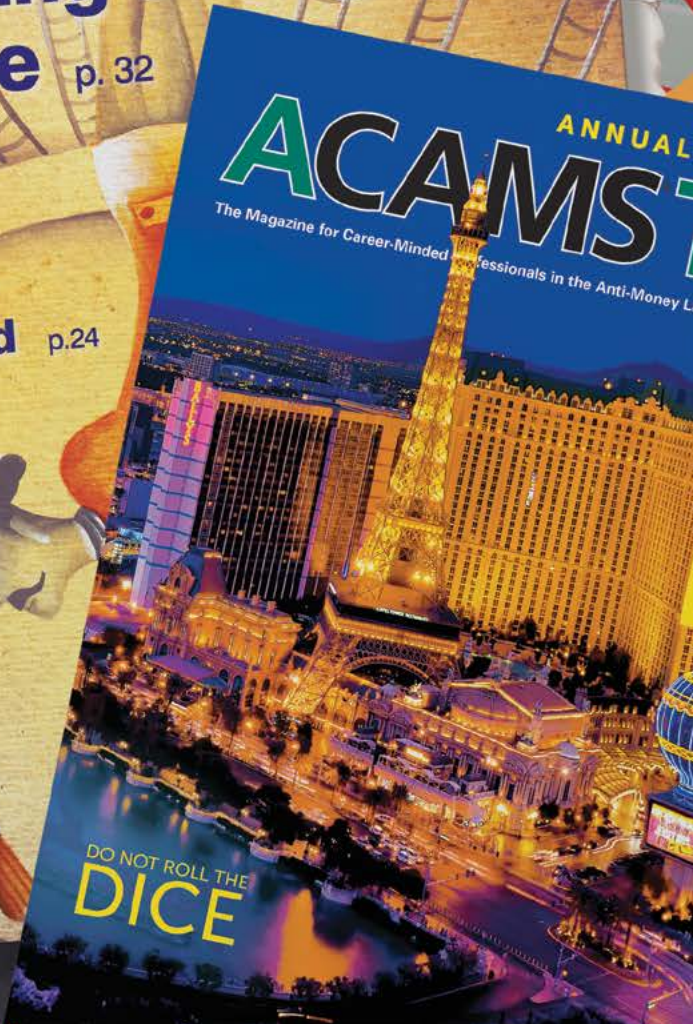
Karla
Karla Monterrosa-Yancey



ACAMSTODAY | SEPTEMBER-NOVEMBER 2011 | WWW.ACAMSTODAY.ORG | ACAMSTODAY.ORG
ACAMSTODAY | SEPTEMBER-NOVEMBER 2011 | WWW.ACAMSTODAY.ORG | ACAMSTODAY.ORG



www.ACAMS.org
www.ACAMS.org/expand





A *CAMS Today* spoke with Karla Monterrosa-Yancey, CAMS, the editor-in-chief of the award-winning *ACAMS Today* magazine for the Association of Certified Anti-Money Laundering Specialists (ACAMS), about her role with the magazine and the past 10 years of *ACAMS Today*.

Monterrosa-Yancey is responsible for the *ACAMS Today* editorial department. She oversees the editorial content and production of the *ACAMS Today* magazine in both English and Spanish and the ACAMSToday.org website.

In addition, she manages the *ACAMS Connection* and *ACAMS Conexión*, a biweekly e-newsletter, the ACAMS forums and the ACAMS Membership Career Headquarters.

Monterrosa-Yancey has over 10 years of experience in publication, editing and copywriting, both online and in print. Her editor's column is award winning and under her leadership the *ACAMS Today* has won numerous awards in both content and design.

Prior to joining ACAMS, Monterrosa-Yancey worked in the accounting, education and technology industries. Monterrosa-Yancey received her Certified Anti-Money Laundering Specialist certification in 2008. She is fluent in Spanish and French, and holds a bachelor's degree in international relations and a master's degree in business administration.

ACAMS Today: As the editor-in-chief, can you describe the role you play at your magazine?

Karla Monterrosa-Yancey: Do you have an hour or two? We could discuss this all day. My role is to oversee the entire production of the magazine from beginning to end. This starts months before each edition is published. I work

with the editorial committee to formulate an editorial calendar for the upcoming year and we meet a few months before each edition drops to discuss the current state of financial crime prevention. I then oversee the editing, design, printing and fulfillment process along with the online magazine and the Spanish editions of the magazine. Did I mention we also publish the magazine in Chinese? Karen Yau from our Asia team oversees this process. Of course, the entire magazine comes to life with the assistance of many. First and foremost our members who contribute articles, our designer, Victoria Racine, Alexa Serrano, the editorial assistant, John J. Byrne, ACAMS' executive vice president, and many more who I have not mentioned.

AT: Your magazine is based on contributions by members in the compliance field. What is the process contributors go through when submitting articles and what are the guidelines contributors need to follow?

KMY: The process is outlined in our contributors' guidelines document found on ACAMSToday.org. However, it all starts with an idea. Our contributors' ideas, expertise and their commitment to financial crime prevention is what makes the magazine the premier publication for financial crime prevention professionals. Contributors submit a synopsis of their idea or a rough draft of the article, along with their CV. If the article is accepted, it goes through the editorial process. This process entails going back to the author with edits, suggestions, comments and recommendations. Once we complete the editorial process, we decide whether the article should be published online, in print or both.

AT: How do you choose the theme for each issue of ACAMS Today?

KMY: The AML/financial crime prevention field is constantly evolving. Sometimes we choose a theme, but we often have to adapt to what is happening in this exciting and dynamic industry.


AT: You have worked with the magazine for 10 years. What tools or resources help you ensure the magazine maintains fresh and informative content in each issue?

KMY: The Editorial Committee is a great resource. The members of the Editorial Committee are on the front lines and are constantly improving their AML knowledge. Another resource is the ACAMS conferences. My favorite conference is the Annual Conference held in Las Vegas. It is interesting to hear the different perspectives and the challenges the community faces. I also like to stay informed by reading the diverse events being held by our chapters around the world. Each chapter knows best the regional challenges they face and they provide events about those topics for their members. My other favorite place to read about what the community is facing is the ACAMS forums. Many members post questions and receive answers from others in the ACAMS community or they start thought-provoking threads. Finally, moneylaundering.com is a great place to read the current state of AML in the world and the latest regulations and guidances.

AT: What is your proudest achievement with ACAMS Today?

KMY: The opportunity to be a part of something meaningful that is actually helping change the world for the better. I would also have to say the many awards *ACAMS Today* has received for content and design.

AT: What are your goals for the future development of ACAMS Today?

KMY: To maintain the momentum of being the premier magazine for the financial crime prevention professional and to continue to expand our coverage of the different areas where money can be used for financial crime. In addition, I would like to translate the magazine into other languages and add more regional area focus sections. Currently, we have *Aspects of Asia*, *European Connect* and *The MENA Report*. But above all, to be a constant go-to source for our members and other financial crime prevention professionals. 

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

15

184 members spotlighted
in the *ACAMS Today*



75 issues of
ACAMS Today
published
in the last
15 years



19 special editions of
ACAMS Today
published



CONFERENCE



LAW
ENFORCEMENT



WOMEN
IN AML

4 pages—
shortest
ACAMS Today

96 pages—
longest
ACAMS Today

2002

March 2002:
ACAMS publishes its
first *ACAMS Today*

2006

October 2006:
Editor-in-Chief Karla
Monterrosa-Yancey
joins *ACAMS*

2007

September 2007:
ACAMS Today publishes
its first Annual Conference
edition and launches
the Know Your
Chapter section

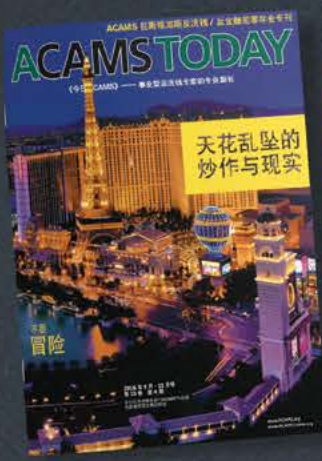
2008

September 2008:
ACAMS Today prints its
first perfect bound issue

September 2008:
Charles Falciglia wins
the first *ACAMS Today*
Article of the Year Award

2010

March 2010:
John Byrne writes
his first EVP letter



14 issues of *ACAMS Today* published in Spanish and Chinese

57 awards won in content and design by *ACAMS Today*



3,184 pages printed



90 published interviews

13 *ACAMS Today* Article of the Year winners

580 AML/CTF professionals contributed to *ACAMS Today*

- 
MarCom Awards
 Association of Marketing and Communication Professionals
- 
Charlie Awards
 Florida Magazine Association
- 
APEX Awards
 Communication Concepts
- 
Tabbies
 Trade Association Business Publications International
- 
AZBEE Awards
 American Society of Business Press Editors
- 
Addys
 American Advertising Federation
- 
Communicator Awards
 Academy of Interactive and Visual Arts
- 
Davey Awards
 Academy of Interactive and Visual Arts

March 2011:
ACAMS Today publishes its first Law Enforcement edition

2011

January 2013:
John Byrne's *AML Now* podcast launches

2013

January 2014:
Editorial Assistant Alexa Serrano joins ACAMS

2014

April 2015:
The redesign of *ACAMSToday.org* launches together with the *ACAMS Today* quizzes

2015

2016

June 2011:
Aspects of Asia section begins

September 2011:
ACAMSToday.org launches

March 2014:
ACAMS Today highlights influential women in AML

April 2014:
ACAMS Today receives its first awards in content and design

June 2015:
ACAMS Today publishes its first Chinese edition

September 2015:
European Connect section launches

December 2016:
The MENA Report section launches

The *ACAMS Today* Editorial Committee took a quick break from their busy schedules to share thoughts, favorite articles and experiences about the *ACAMS Today* magazine. Elaine, Kevin, Amy, Eric, Joe, Brian, Debbie, Ed, Rob and Jennifer have given of their time and expertise as contributing writers and much more, to help keep the ACAMS magazine the premier publication for professionals in the financial crime prevention field. ACAMS would like to thank the Editorial Committee for their continuous service and support in the fight against financial crime and for sharing their knowledge with the ACAMS community.



“My most favorite article comes from the September-November 2016 Annual Conference Edition. I always look forward to this edition because of the diverse topics. The article’s title, “Do Not Roll the Dice” caught my eye and the content intrigued me because my exposure to BSA/AML is primarily with banks.

This article highlighted some similarities with bank AML compliance, but also the unique challenges and differences of AML programs at casinos, such as sources of due diligence information. At casinos, they are able to gather information on their customers via player card programs, the cage and the credit management department for front money accounts. This is a great read if you have not had a chance to see it. Thank you Peter Alvarado and Thomas Paramo for writing it!”

Elaine Yancey, CAMS

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.



“Looking back on my years of writing for and reading *ACAMS Today*, what I really value are the member profiles. ACAMS members toil in relative anonymity, performing vitally important work. Recognizing ACAMS members is a small, but notable step toward giving the compliance professional and their work the visibility they deserve.”

Eric Sohn, CAMS

AN INTERLUDE WITH THE ACAMS TODAY EDITORIAL COMMITTEE



“My favorite article is one I wrote almost five years ago titled “Balancing Your Career and Education—A Professional’s Guide to CAMS Exam Preparation.” As the ACAMS community continues to expand, there are many who are looking to take the CAMS exam who may have forgotten—or never even learned—

how to study for an exam. I have had more people from around the world reach out to me about this one article than any of the other articles I have written for *ACAMS Today*. The responses I have received on this article demonstrate some of the most important things about what ACAMS is all about: sharing knowledge and connecting with each other on a more personal level to help the entire membership become better professionals. The feedback I have received continues to inspire me to volunteer with ACAMS, because I know that it helps others. While I do not directly investigate crimes or bring criminals to justice, I feel that I have been able to make a small contribution to the overall ACAMS community—and that is what the organization is all about.”

Kevin Anderson, CAMS



“The level of anticipation I experience while waiting for each new issue of *ACAMS Today* to be published is eclipsed only by the level of excitement when I read the issue’s table of contents. Each issue is packed full of good information. Some of the information I digest in every issue is used immediately in my current

role, and other information may be nuggets of gold that I file away for future roles/responsibilities. The articles I most appreciate are those that provide guidance or tips on how to implement an AML program like “The Why and How of Writing a No-SAR Justification” written by Brian Arrington, Don Temple and Ed Beemer in the March-May 2014 edition. This no-nonsense writing style filled with useful information is exactly what I seek from an industry magazine and it is exactly what I get from *ACAMS Today*. Bravo!”

Amy Wotapka, CAMS



“Human Trafficking: If You See Something, Say Something” is my favorite article because it brings to light a horrible subject that requires all of our attention and diligence to prevent as citizens of the global community and as anti-money laundering (AML) compliance specialists and law enforcement. I believe that the trafficking of humans for any criminal enterprise is one of the most horrible things that can be perpetrated upon another person—it is at its core a modern form of slavery. The AML profession offers one of the most direct opportunities whereby we can work to eliminate this problem in society. We have the tools to ensure that we can identify, monitor and report the warning signs of human trafficking activities by “following the money.” I hope that those best familiar with the issue of human trafficking continue to contribute to *ACAMS Today* in the years ahead, so that we all can remain vigilant in the fight against this problem.”

Brian Arrington, CAMS



“My time on the *ACAMS Today* Editorial Committee has provided me with a wealth of ideas and knowledge far beyond what finally appears in print. I glean so much from the discussions during our quarterly meetings when article ideas—or even the glimmer of ideas—are thrown out, debated, added to and subtracted from until the basis for an article takes shape. It is fascinating to watch these wisps of thought evolve into articles, webinars and the occasional white paper. I am privileged to work with the talented and dedicated people who have served on the Editorial Committee over the years.”

Debbie Hitzeroth, CAMS-FCI



“Whenever I contribute to *ACAMS Today*, I almost always take the perspective of the compliance officer. In my opinion, they have the toughest job in the anti-money laundering industry, usually laden with responsibility and often resource poor. I think that anytime the magazine offers compliance officers ideas, insight or knowledge to make their job easier, more efficient, or more effective, it has fulfilled its most important mission.”

Ed Beemer, CAMS-FCI



“*ACAMS Today* is always very current in the topics it covers and it provides AML and compliance professionals with a great collection of articles relevant to the anti-financial crime community.”

Jennifer Hanley-Giersch, CAMS



“The articles from *ACAMS Today* I enjoy reading the most are ones written by current and former law enforcement (LE) professionals. As a banker, it is interesting to read LE’s view on Bank Secrecy Act/anti-money laundering (BSA/AML) and how they use the reports we as bankers file to assist them in their investigations. I also like to read through those articles to see if I can pick up possible transactional activity or scenarios that I could possibly utilize in our AML system to see if the activity they point out may uncover any activity I may need to investigate.”

One particular article that comes to mind was written by Steve Gurdak. His article “Talk the AML Talk” was published in the June-August 2015 Fifth Law Enforcement edition of *ACAMS Today*. It goes through BSA/AML interviewing and it is directed mostly at the private sector BSA/AML departments. The article gives well-thought-out examples on why BSA/AML teams (or tasked bank staff) should reach out to customers more to help gather information on cases.”

Joe Soniat, CAMS-FCI



“I have been CAMS certified for over a decade and have watched the CAMS certification become the Gold standard for certification in the financial crimes profession. While participating as a founding member of the ACAMS Carolinas Chapter board, the *ACAMS Today* Editorial Committee and the Educational Task Force, the most valuable result of those and other activities is the knowledge that I have gained from being in contact with the diverse range of professionals in the ACAMS financial crimes community. As president of NominoData, a data solution company, I have found it personally fulfilling to help those colleagues in the ACAMS community to meet their business needs.”

Robert Goldfinger, CAMS

Editor’s note: For more information on the Editorial Committee, please visit ACAMSToday.org.

A SARS AND STRIPS RETROSPECTIVE

Cartoons have long been used as a communication tool for conveying information succinctly and effectively. The modern format of cartoons usually involves satire, humor and/or caricature to highlight a core message. Applying this method of reaching out to the international anti-money laundering (AML) community has been successful and has given rise to this retrospective of cartoons from the past few years.

Many years ago, I began working with Grant Brownrigg of Grantland, a very successful and respected business cartoonist. Over the years, we developed a successful collaboration combining my technical and communication knowledge with Brownrigg's artistic and wordsmithing skills. The team of Beemer and Brownrigg had a very successful run providing cartoons and comic videos to the U.S. Army to help drive home key messages on information assurance and cyber security. The work we did was formally recognized

by the U.S. government for its effective communication on these topics. When I broached the subject of providing an AML cartoon for *ACAMS Today* to Editor-in-Chief Karla Monterrosa-Yancey a few years back, she graciously agreed to give it a try. Happily, the resulting work has been popular with *ACAMS Today* readers.

Our approach has always been that when you have a simple key message or concept to pass along to a wide audience, a cartoon is often the perfect tool. Formal announcements are often overlooked or not committed to memory. Yet, a cartoon will appeal to today's short attention span and provides a visual or humorous "hook" to instill the message.

Producing a four-panel cartoon four times a year would seem like a simple task. However, creating a cartoon for the international AML community is more challenging than one might expect. This is especially true in crafting

words and images that are understandable and acceptable to a diverse international audience. However, while the humor might seem simplistic at times, the cartoon has been popular and we are very pleased we can continue contributing to the magazine.

This retrospective of some of the more popular cartoons over the past few years is an honor. We have added a few notes to each one to provide insight into its concept and development. We hope the AT audience continues to enjoy our efforts to make key AML messages a little more fun to digest. 📄

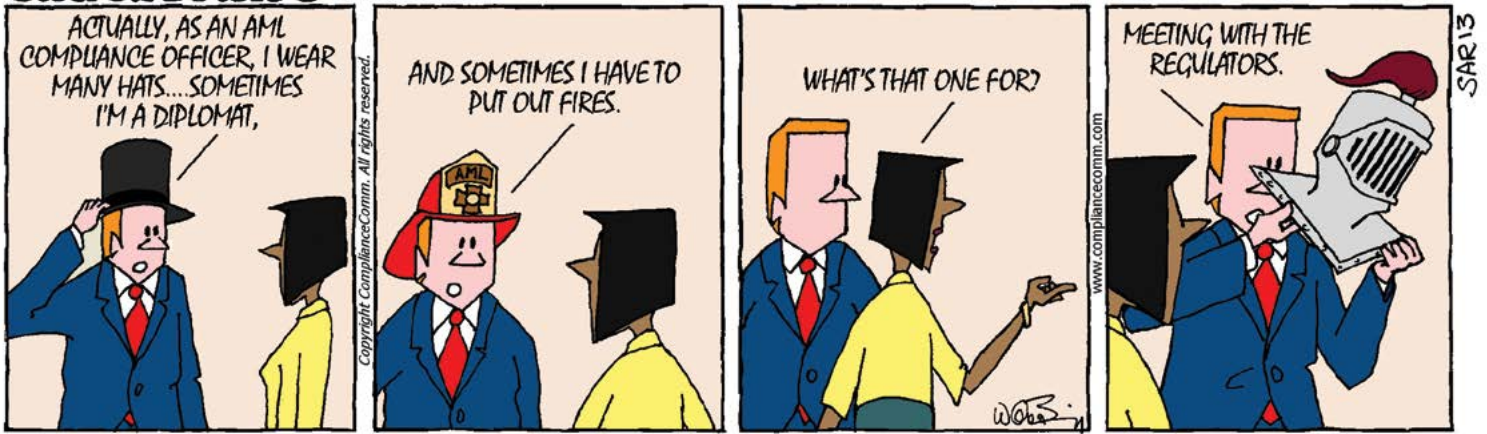
Ed Beemer, CAMS-FCI, APR, principal, CorpComm Solutions LLC/ ComplianceComm, Arlington, VA, USA, efb@compliancecomm.com

Grant Brownrigg—Grantland Cartoons, www.grantland.net, Charlottesville, VA, USA



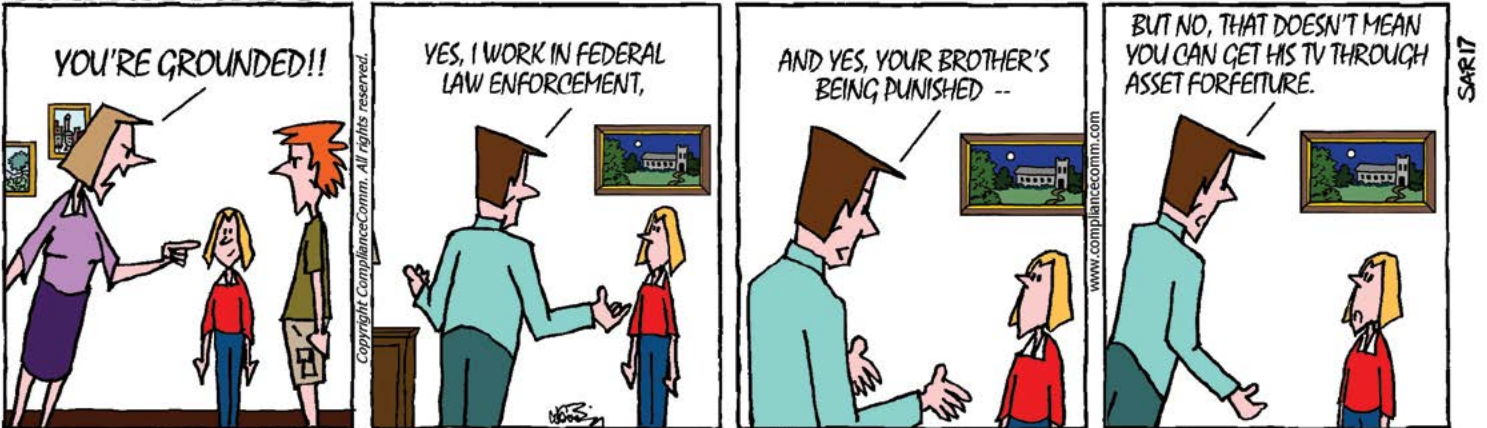
The cartoons often approach a message from a BSA compliance officer's point of view. We just count on the regulatory community having a keen sense of humor.

SARSTRIPS™



The artist thought this was the best humor of all these cartoons. Some AML professionals thought it was pretty accurate.

SARSTRIPS™



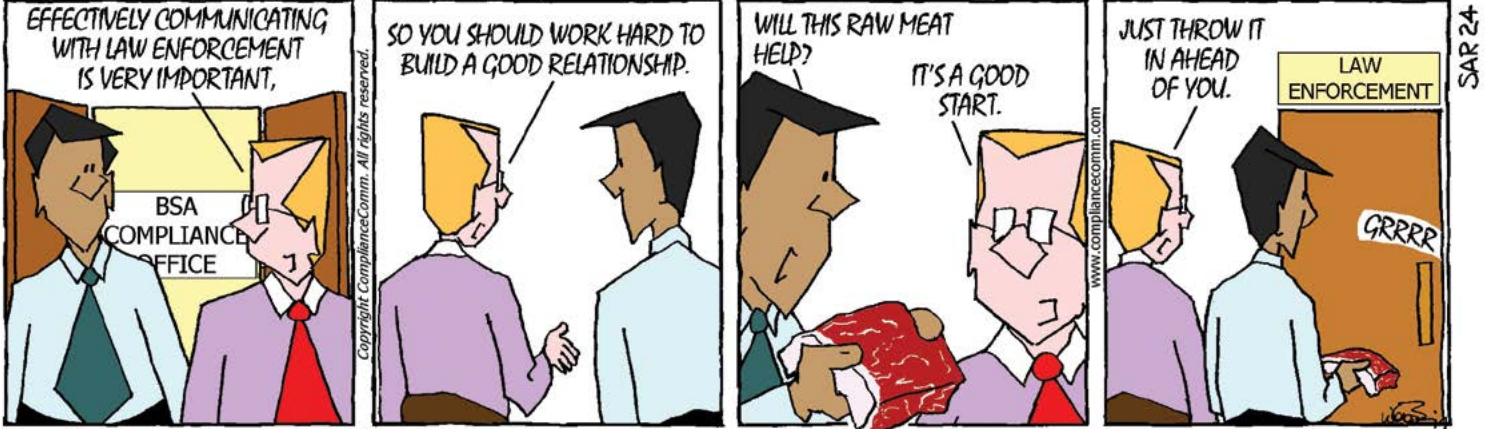
Parents in law enforcement should remember that kids are quick to grab on to a concept.

SARSTRIPS™



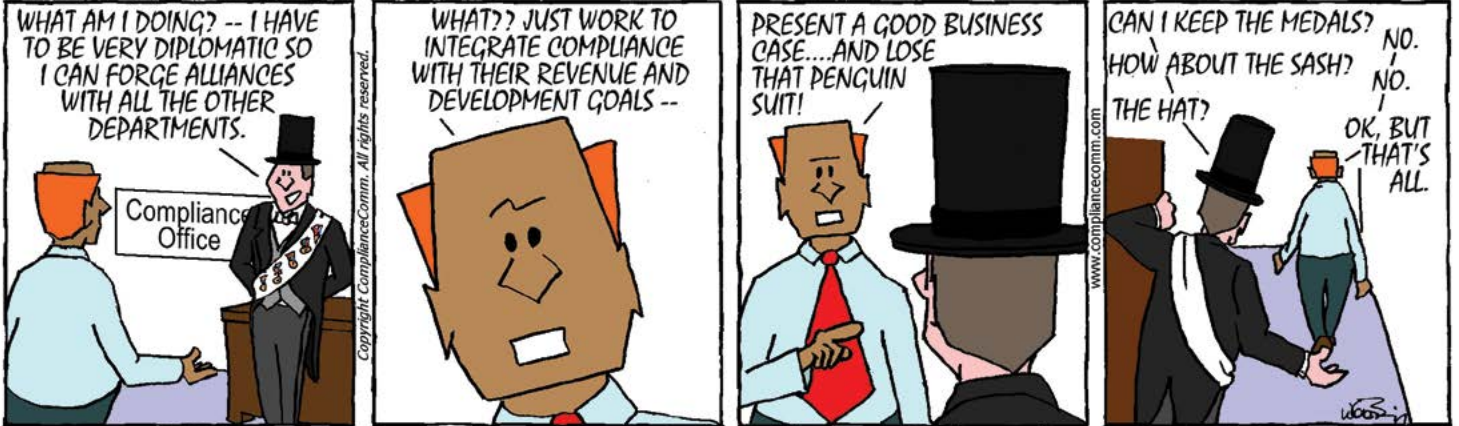
How many times do we AML types have trouble "leaving it at the office?"

SARSTRIPS™



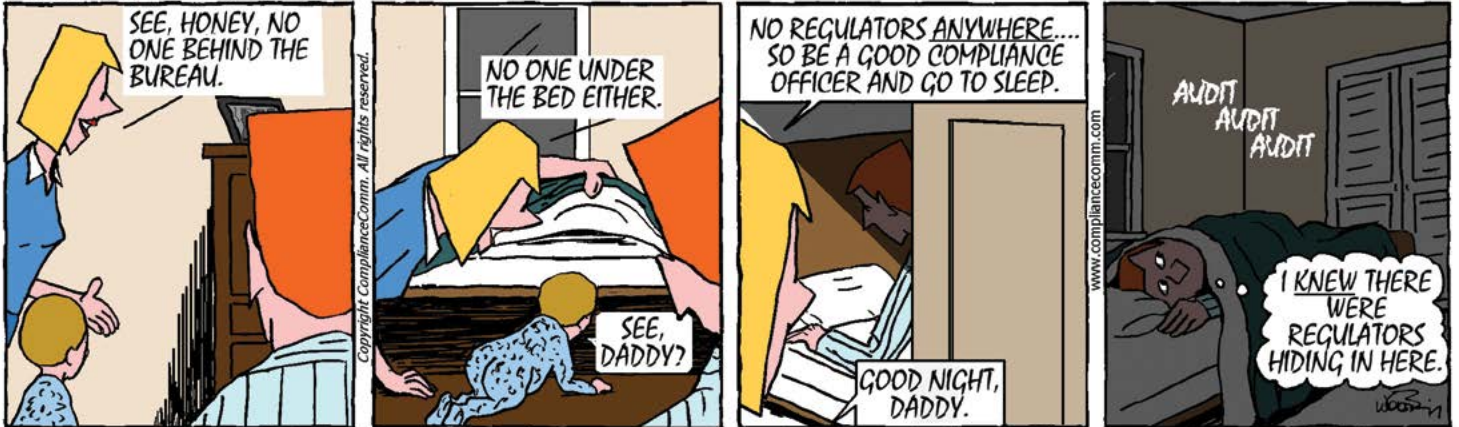
We often wonder what law enforcement officers think about compliance officers.

SARSTRIPS™



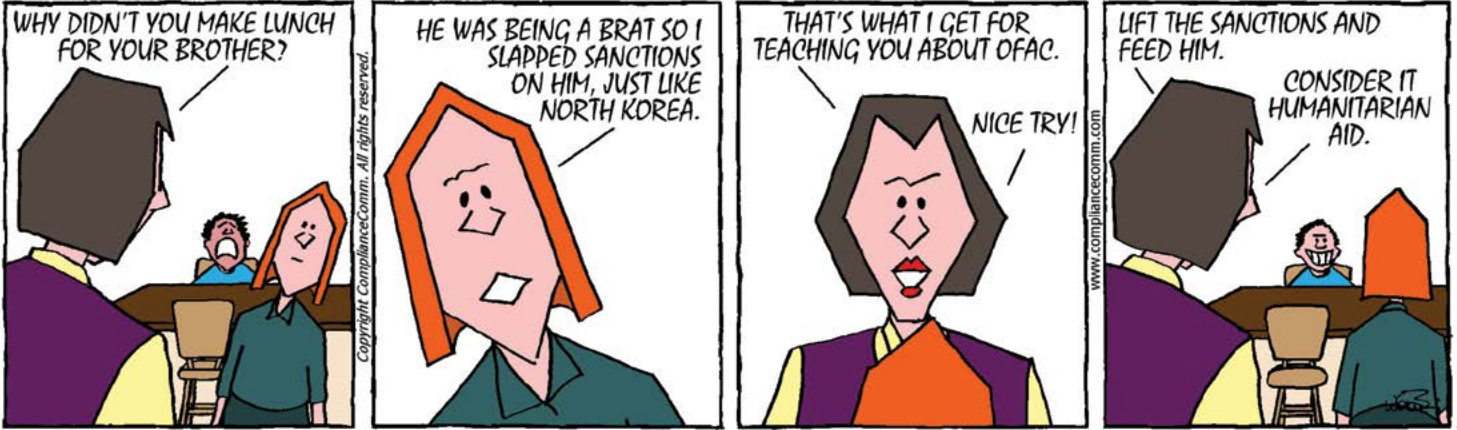
Good negotiating skills are often more useful than a good hat in the AML world. But who does not appreciate a good hat?

SARSTRIPS™



This was a classic switch with the kid helping to dispel the parent's fear. For us, our closets are filled with editors.

SARSnSTRIPS™



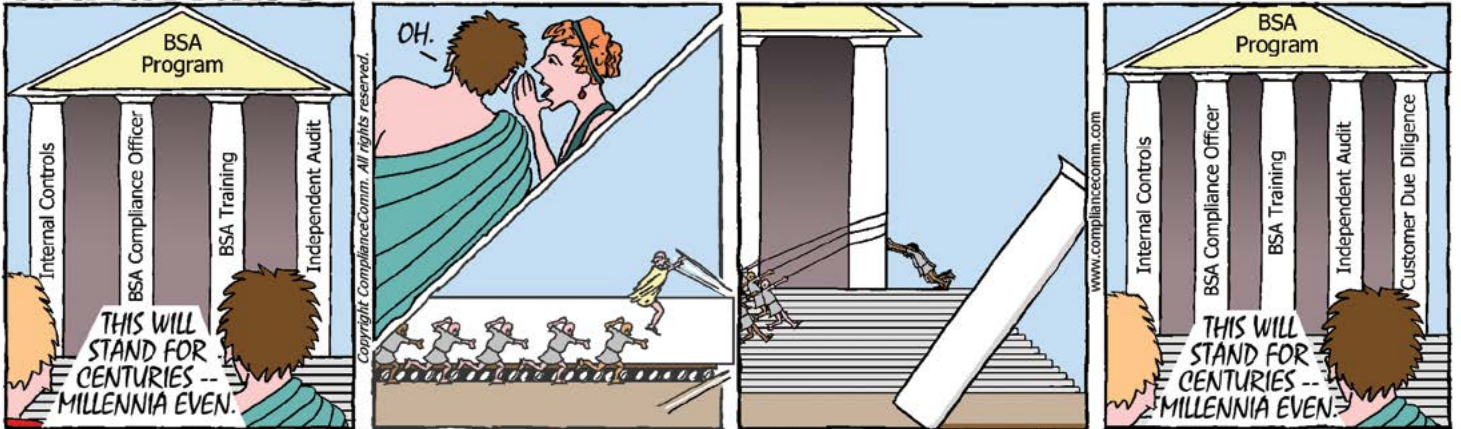
We love using family situations to shed light on work issues.

SARSnSTRIPS™



We bet there is not a BSA analyst out there that would not mind doing some undercover work.

SARSnSTRIPS™



Let us just say this took a little longer than normal to draw.

GOLDEN OLDIES FROM ACAMS TODAY

MEMBER CONTRIBUTION

The circus that is post 9/11 AML compliance

Edward Monahan, CAMS, an editorial task force member, works at PricewaterhouseCoopers in Boston. He can be reached at: edward.monahan@us.pwc.com

There is an uncanny resemblance between preparations for today's anti-money laundering regulatory examinations and the classic repertoire of an accomplished circus act, I've found.

There are acrobats (financial institutions) juggling multiple, moving objects (recordkeeping, reporting, risk assessment, monitoring, auditing, testing) taking care not to lose balance on a jittery tight-rope (policies, procedures, understaffed compliance) exhibiting their mastery (of anti-money laundering regulations) for a chorus of critical spectators (management, regulators, customers). And it really does make for quite the event.

Moving Objects: Keeping All Pieces in the Air

Preparing for Bank Secrecy Act/AML regulatory assessments is an extremely delicate balancing act – the moving objects are constantly being juggled around and as always, if one falls, the entire act goes to pieces under the unforgiving glare of intense and targeted examiner focus.

New Customer Identification Program (CIP) rules bespouse risk-focused customer monitoring and the front-end challenges are enormous – gathering, checking, evaluating and testing information on all customers across multiple accounts and products tends to send sales staffs to the brink and stretch compliance risk management beyond previous limits. Yet, if done poorly, subsequent monitoring efforts are inevitably flawed.

The monitoring itself must be consistent, creative and flexible. Know Your Customer (KYC) monitoring need to be relationship – not acquaintanceship – based and it is definitely not enough to perform KYC just at the start of a relationship because the rules now say that ongoing CIP is the new standard.

Tight-Rope: Balanced Footing Under the Spotlight

The tight rope itself is narrow and un-

stable and judgmental spectators expect that compliance officers breeze through with an air of competence and sprezzatura, exhibiting a seamless integration of post-9/11 Patriot Act requirements.

But AML regulations require that risk management be based on policies and procedures that provide clear, concise, detailed and updated guidelines for aligning CIP, monitoring and testing programs to an institution's specific customer base, internal controls, resources, and business activities and ensuring that policies lead to useful, specific procedures is no easy task.

Institutions have little room for error – the difference between soaring above the audience and crashing into the spectators is razor thin.

Just as the high-wire artist invests thousands of practice hours to achieve effortless balance high above the spectators, so too must institutions dedicate resources, time and management talent to very basic policy and procedural implementation.

CIP, KYC and monitoring are balanced steps along a narrow high-wire: compliance testing and appropriate internal audit scope and practice are necessary to complete the balanced performance. Risk-neutral CIP or untested monitoring are costly mis-steps that can bring a high-flying compliance performer crashing down.

Loud Chorus: Spectators and Participants

In the post-9/11 Patriot Act environment, regulatory agencies and BSA/AML examiners have come under intense pressure to forestall terrorist financing by preemptive examinations of AML regulatory compliance and testing.

And even though examiners and boards appreciate the high risks of doing business against the backdrop of money laundering, terrorism and cyber-enabled transaction processing, they are brutally unforgiving of clumsy efforts to manage

financial crime risks with poorly designed compliance programs, unqualified staff and inadequate senior management oversight.

Institutions have little room for error – the difference between soaring above the audience and crashing into the spectators is razor thin. AML examination scope, schedule and reporting are accelerated and intense. Institutions that fail to risk-rate customers or monitor according to coherent, contemporary procedures are rarely given a second chance to correct basic compliance failures.

Exposure of corporate directors to individual liability places corresponding pressure on Boards to oversee, manage and remediate problems before examiners uncover significant AML compliance deficiencies. And recent high profile enforcement actions that have led to major civil money penalties highlight the pressure upon examiners to enforce comprehensive AML regulations before embarrassing evidence of regulator oversight might occur.

The post-9/11 Patriot Act environment has transformed AML compliance from reactive procedures, recordkeeping and routinized KYC to risk-driven financial intelligence that supports a complex balance of monitoring, testing and preemption.

In the past a juggler or tight-rope walker might get by with a single, practiced skill. However, now an audience demands much more of the same performer.

Multiple AML control risks must be managed and balanced on a high-wire of examiner expectation. AML regulatory readiness requires competency, practice and experience. It is a process of progressive mastery that, while repeated time and again, is ever subject to persistent risk of inattention, loss of balance and swift, steep, crashing failure.

Finally, the chorus itself is diverse and demanding with each spectator critiquing the act from a different viewpoint. Needless to say, shaky performers don't last long, and audiences are unforgiving.

Making the transition from the public to private sector

Many of us in the anti-money laundering (AML) profession have left law enforcement careers in the public sector, moving from a world of public service to a world dictated by revenue production — or revenue protection through loss prevention. Both of us made this transition to the business world, and our goal with this article is to provide an overview of our experience in moving from the public to private sector and to offer some advice on how to do it effectively.

Do your homework

Well in advance of making your move, one of your top priorities before leaving a public sector career should be to do your homework. Meet with individuals who have already made the transition and explore with them the pro's and con's of the change. Plus, try to ensure that whatever company you are considering joining has a culture that is fully compatible with your own work ethic.

Be driven

At the outset, it is important to remember that the private sector values individuals with an entrepreneurial bent, a drive to succeed. The co-authors of this article were successful in our police organizations, enabling us to rise through the ranks. We both reached senior executive positions, where we attained visible leadership roles. We both represented our organizations with the media and through speaking engagements at governmental and business forums. In fact, we first met in 2002 when we represented our countries at a European Union law enforcement conference in Ireland. We also enjoyed the opportunity to establish a network of contacts in both public and private arenas throughout the world. Our extensive investigative experience in law enforcement provided us with a solid foundation for our transition to the private sector.

Capitalize on strengths

Capitalizing on strengths has been important in establishing our consulting careers. Interviewing skills and the ability to assess body language, verbal cues and micro-facial expression are capacities

welcomed by potential clients. Experience in understanding the criminal mindset in exploiting the financial system is an attribute of real value to financial businesses. We also had undercover experience, which helped hone our people skills. What's important is recognizing and identifying the value of your experience to potential private sector clients.

Training

Despite our extensive law enforcement backgrounds, we had to confront gaps in our understanding of the way the private sector operates. We quickly learned how little we really knew about the internal workings of financial institutions and, perhaps more important, their perspective on Bank Secrecy Act reporting requirements.

We realized we needed to apply our law enforcement strengths to the private sector in a constructive manner. We also recognized the importance of attending as many conferences as we could to better understand the industry perspective and identify the issues that resonated most extensively with the industry. The industry conferences also provided an excellent vehicle to network and enhance professional relationships.

Develop critical characteristics

Our transitions to the private sector were greatly facilitated by characteristics we developed throughout our law enforcement careers, such as commitment, purpose and ethical grounding. A critical attribute is the ability to listen. In our opinion, this is one of the most important skills necessary to provide clients with the services that meet their specific needs.

Many law enforcement professionals gravitate to investigative positions in financial institutions. Their experience and ability to understand the criminal mind and how criminals exploit the system, coupled with the ability to conduct interviews, investigations and collect evidence, smooth their transition into the banking environment. Other former law enforcement professionals join consulting firms or provide individual consulting services drawing on their experience to add value to their client services.



A strong network of former law enforcement personnel keep in touch and, on a project-by-project basis, join skill sets through subcontracting arrangements to meet the needs of their clients. Working in conjunction with this network eases the transition process.

Ethics

Ethics is of extreme importance to the financial community. Having a background where ethics was not only discussed but was engrained as a part of professional routine enables us to factor ethics into whatever services we perform. As in law enforcement, credibility and reputation are of paramount importance.

For both of us, it has been reassuring to know there is life after law enforcement. We have been fortunate in making the transition from the public to private sector and developing a niche for ourselves that is challenging and rewarding. **A**

Dennis Lormel, managing director Northeast region, IPSA International, Toronto, Canada, DLormel@ipsaintl.com

Garry Clement, managing director, IPSA International, Toronto, Canada, garryip-saintl@plornet.com

Barbarians at the gate

—The danger of mortgage fraud

California surfing, New York's Broadway, Colorado Rockies and Florida's sunshine are each known for their unique features; however, they all now share a plague. They are ranked as among states with the highest amount of reported mortgage fraud in the U.S. in 2008, according to the FBI's Mortgage Fraud report released July 7, 2009.¹

Suspicious Activity Reports (SARs)² increased 36 percent to 63,713 during fiscal year 2008, compared to 46,717 reports in 2007. While the total dollar loss attributed to mortgage fraud is unknown, financial institutions reported losses of at least \$1.4 billion, an increase of 83.4 percent from 2007.

Nationally, more than 3.1 million foreclosure filings were reported on approximately 2.3 million properties during 2008, up 81 percent from 2007 and a whopping 225 percent from 2006.³

The first half of 2009 intensified as the Financial Crimes Enforcement Network (FinCEN)⁴ ranked the top 10 states for SAR filings as: California, Florida, New York, Illinois, Georgia, Texas, Arizona, Michigan, Virginia and New Jersey. Overall, the borrower stands alone in the number one position as the main suspect with the mortgage broker further away in second place. The top fraud issues include forged documents, debt elimination or foreclosure rescue schemes, Social Security Number issues, misrepresented assets or undisclosed liabilities, title or insurance concerns and appraisal matters.

As 2010 ushers in a whole new earthly creation of mortgage loan fraud, the leftovers of the cheating trends from the not so distant past linger.

In a short sale, the current fraudster delight on the mortgage fraud menu, the borrower will obtain funding for a property and most likely place a Home Equity Line of Credit (HELOC) on the subject concurrently or shortly after the closing. The property value may have been deliberately inflated in order to obtain a higher limit of HELOC funds for the taking. Not surprisingly, the borrower defaults on the loan after making a few payments or none at all. Avoiding the mortgage company's attempted contacts and just before foreclosure, the borrower reaches out to the lender and conveys that the loan is no longer affordable. When given the opportunity by the mortgagor, the borrower purposely does not qualify for a work out package.

This structure would have allowed a qualified borrower to catch up with their mortgage payments. From the perpetrator's point of view, the motive removes a lender's option and eats away time to this draining piece of property. Precisely at this moment the ruse wanders into the picture disguised as a prospective buyer, who is actually a friend, relative, or business associate of the borrower. This relationship is not disclosed and the co-conspirator offers a low-ball amount that grossly undercuts the property resale price. After the short sale transaction is negotiated and complete, shortly thereafter, the new owner will sell/convey the property back to the original borrower and voila, this fraudster just swindled a \$300,000 residence for \$57,000, most likely with minimal expenses or payoffs.

Lending institutions, with the click of a button, can tap into public records databases prior to the short sale to connect any players or, eliminate suspicion.

There are a few all-inclusive web sites out there that are quite reliable. For further recourse, follow up on closed short sales can be conducted by checking deeds filed with the county recorder or spot checking the vesting history to see if any concerning ownership changes transpired.

The additional deception associated with a fraudulent short sale also should not be underestimated. Many lenders do not permit certain parties to a loan to be connected, unless this information is disclosed in writing and accepted by all parties. If this occurs it is considered to be an Undisclosed Non Arms Length transaction (NAL). This method is intentional, deceitful, used for personal financial gain and therefore subject to a SAR filing.

Investigation methods have not changed just increased in volume. The course of action is as stale as that lost piece of bread hidden in the cabinet — follow the money.

The fact is that mortgage loan deception is not going away anytime soon and the lending industry can not face this disease alone. Mortgage fraud units are part of every branch of law enforcement with new interventions taking root on a regular basis.

According to FinCEN⁵, in April 2009, the Departments of Justice (DOJ), Treasury, Housing and Urban Development (HUD), and the Securities and Exchange Commission (SEC) announced the formation of an interagency Financial Fraud Enforcement Task Force to strengthen efforts to combat financial crime. The task force's leadership, along with representatives from a wide range of federal agencies, regulatory authorities and inspectors general, will work with state and local partners to investigate and

¹FBI Issues 2008 Mortgage Fraud Report, http://www.fbi.gov/pressrel/pressrel09/mortgage_070709.htm

²FBI Issues 2008 Mortgage Fraud Report, http://www.fbi.gov/pressrel/pressrel09/mortgage_070709.htm

³FBI Issues 2008 Mortgage Fraud Report, http://www.fbi.gov/pressrel/pressrel09/mortgage_070709.htm

⁴FinCEN, SAR Activity Review – Trends, Tips & Issues, Issue 16, 10/2009, http://www.fincen.gov/news_room/rp/files/sar_tti_16.pdf

⁵FinCEN, Annual Report Fiscal Year 2009, http://www.fincen.gov/news_room/rp/files/YEreport/FY2009/annualreport.html

prosecute significant financial crimes, ensure just and effective punishment for those who perpetrate financial crimes and recover proceeds for victims. Three months after its inception the “Treasury’s Financial Fraud Enforcement Task Force has pursued more than 100 cases,” cracking down on mortgage fraud and shutting down suspect companies.

As this fraud-guard continues to strengthen, government agencies will be able to better curb mortgage loan abuse by coordinating information and focusing resources in their fraud investigations, which will aid in the reduction of mortgage loan fraud. This includes alerting financial institutions to emerging schemes, stepping up enforcement of the various types of mortgage fraud, and educating consumers to avoid becoming the victim.

Accurate SAR filings are an important measure as it allows law enforcement to focus on infectious geographical areas and the types of trendy issues at hand. Such awareness will better equip the industry as a whole to fight mortgage fraud. **A**

Stacey Kerreos, SAR manager, GreenPoint Mortgage Funding, Inc., Larkspur, California, USA, California Licensed Private Investigator, Stacey.Kerreos@greenpoint.com

HIDING IN PLAIN SIGHT

CHALLENGES IN THE
IDENTIFICATION OF
ULTIMATE BENEFICIAL
OWNERS AND
TRADE-BASED MONEY
LAUNDERING IN
INDIAN CONTEXT

Illicit financial flows through developing countries due to trade-based money laundering (TBML) is one of the most pressing challenges facing policymakers across the globe and India is no exception. The Financial Action Task Force (FATF) “defines TBML as the process of disguising the proceeds of crime and moving value through the use of trade transactions, in an attempt to legitimize their illegal origins” or to finance their activities.¹

One must note that the most important and basic element of carrying money laundering (ML) activity through TBML is the use of benami accounts or accounts that are opened in one name but are controlled by others. Once the criminals or so-called money launderers are able to open benami accounts (by breaking the know your customer/customer due diligence (KYC/CDD)-related shield of any bank or authorized institution), carrying TBML-associated activity will be much simpler to execute.

Regulators across the globe are cognizant of this and are increasingly focusing on fine-tuning their KYC/CDD and transaction monitoring-related regulatory framework to tackle the usage of network of third parties and remittances to and from multiple accounts, which ultimately will help in restricting the menace of TBML.

In India, Reserve Bank of India (RBI) has also been working very hard toward formulating enhanced measures to tackle the issues around TBML.

Some notable regulatory changes and guidelines issued in recent times impacting TBML include:

- The passing of the Undisclosed Foreign Income and Assets (Black Money) and Imposition of Tax Act, 2015 and Benami Transactions (Prohibition) Amendment Act, 2015. Clause 177 of the 2015 Finance Bill proposed to club all offenses under

Section 132 of the Customs Act, such as false declarations, false documentation, etc., as offenses under the Prevention of Money Laundering Act (PMLA), 2002.

- Forming an elite panel to devise and solidify indicators (on classification of certain types of transactions), evaluate and identify red flags, in the case of any misdemeanor.
- The Indian financial intelligence unit rolled out a new process mandating all banking and financial institutions to file formatted cross-border wire transfer reports for amounts exceeding INR 5 lakh.²

The relevance of these changes can be clearly seen in one of the biggest Forex scams which was brought to the attention of RBI in February 2015. This scam is a classic example where three typologies (AML, TBML and Forex scams) can be noticed in one single incidence or event.

As per the media reports and public statements made by RBI, the scam was a result of several irregularities in one of the biggest public sector banks' transactions where illegal transfers of approximately \$6.17 billion in foreign exchange were being made to Hong Kong through newly-opened accounts in one of the bank's branches located in Delhi.

The overall modus operandi of the scam exploited two main loopholes of the existing Indian regulations. The first loophole pertains to the duty drawback scheme where several bogus/shell companies or individuals exported goods at a higher price to their own fake companies to take benefit of the duty drawback scheme of the government. The second loophole pertains to regulations for advance remittances for imports. The modus operandi followed was that a number of current accounts were opened in the branch. As per the Indian banking system, “a remittance of up to \$100,000 does not raise an alarm and is automatically cleared without supporting documents of imports. The money launderers exploited this loophole to pass under the radar.” They also “selected commodities that are prone

¹ Vikram Babbar, “Trade-based money laundering—A macro view of the changing dynamics,” Forensic Diaries: A Fraud Investigation and Dispute Services Blog, May 27, 2016, <https://forensicdiariesblog.ey.com/2016/05/27/trade-based-money-laundering-a-macro-view-of-the-changing-dynamics/>

² Ibid.

to cancellations on account of quality or sharp price fluctuations like fruits, pulses and rice.”³

The entire scam highlights the following stark irregularities:

- Current accounts have been opened by several entities with banks, often even without fulfilling the KYC requirements and appropriate risk categorization.
- The entries for remittances—many of which were done manually—have allegedly been fudged and many of them have been made by punching the exchange rate as 0.0001 rupees to a dollar when the prevailing exchange rate was 60 rupees to a dollar.”⁴
- Docket numbers were not obtained/generated for each remittance and despite heavy advance payments for imports being made to the same suppliers, suppliers’ credit reports were not obtained.
- Required trade transaction documentation was not completed.
- In most cases, the mode of shipment, date of shipment and the place of shipment were not mentioned in the pro forma invoice and the “bill of entry/evidence of imports was not obtained before making further remittances to the same supplier.”⁵ No effort was made by the bank to obtain evidence of import/bill of entry from importers.
- “Advance import remittances have been permitted without verifying the bonafide of transactions and without carrying out proper due diligence of both the Indian clients as well as overseas suppliers.”⁶

The case study clearly evidences the fact that TBML is a high-risk area of business, which is used for carrying out ML-related activities. Some of the key

challenges, which are mirrored by the above case study, are mentioned below:

- Ineffective implementation of KYC and CDD policy and procedures
- Non-identification of red flags and inadequate enhanced due diligence
- Delay in regulatory reporting
- Employees not adequately qualified or knowledgeable
- Ineffective internal controls framework


The previously mentioned cases and the challenges enumerated prove that the risk arising from trade finance activities and the rise in the number of entities participating in international trade, is a daunting task for banks and financial institutions operating in India. To safeguard themselves from the challenges previously highlighted, bankers need to consider the following key pillars of TBML preventive mechanisms:

- *Policies and procedures*—AML and compliance policies and procedures should contain a clear process for identifying and verifying the ultimate beneficial owner (UBO). All new and existing accounts are subject to verifying and identifying UBOs during account opening or KYC update processes.⁷
- *Identification of red flags*—Bankers should timely identify the red flags to ensure timely escalation and investigation of the red flags identified.
- *Qualified and trained staff*—Employees that obtain identification and perform the verification of the UBO should be qualified and have an understanding of how to deal with legal entities and how to track the UBO in complex structures that may be located in offshore jurisdictions (Cayman Islands, Panama, etc.).

- *Quality control and quality audits*—The tests and assessments conducted by quality control and auditors should be robust enough in assessing the weakness of current processes and the opportunities for control enhancement.

These preventive measures, if implemented appropriately, will surely assist in the global effort to curb ML via TBML. One must note that with an ever-increasing economic growth, TBML is gaining importance given the growth in world trade and there is a rapid rise in the volume of trade transactions handled by banks and financial institutions. This will have its own challenges in terms of increasing diversion and the flow of illicit funds into TBML.

Banks in India face a similar set of concerns with TBML and one of the root causes is the lack of sufficient KYC data or due diligence, carried out by the operations staff at bank branches at the time of account opening, execution of import export transactions and monitoring.⁸

Hence, strengthening the KYC/CDD framework with a clear focus on identification and verification of UBOs is paramount to curb ML via TBML. Strong AML programs and adequate knowledge becomes critical in order to avoid being confused by highly complex, multilayering and shady offshore entities designed to hide the identity of UBOs. Specialized knowledge, qualified staff, inadequate compliance policies and procedures are some challenges to face. Unless these challenges are addressed at a domestic, as well as at an international level, success in tackling TBML activities would be minimal. 

Sachin Shah, CAMS, vice president, HSBC, Mumbai, India, sachin.shah@hsbc.co.in

³ Shishir Asthana, “5 Things to Know about the Bank of Baroda Forex Scam,” *Business Standard*, October 15, 2015, http://www.business-standard.com/article/companies/5-things-to-know-about-the-bank-of-baroda-forex-scam-115101500367_1.html

⁴ “Bank of Baroda finds RS 6,000 crore of illegal forex transfers,” *Times of India*, October 10, 2015, <http://timesofindia.indiatimes.com/business/india-business/Bank-of-Baroda-finds-Rs-6000-crore-of-illegal-forex-transfers/articleshow/49295338.cms>

⁵ Ibid.

⁶ “BoB forex scam: RBI finds irregularities in banks’ transactions,” *The Hindu Business Line*, February 15, 2016, <http://www.thehindubusinessline.com/money-and-banking/bob-forex-scam-rbi-finds-irregularities-in-banks-transactions/article8240677.ece>

⁷ Alaa Saleh Ghaith, “Ultimate Beneficial Owners (UBO) Between Identification and Verification,” ACAMS, 2016, http://files.acams.org/pdfs/2016/Ultimate_Beneficial_Owners_A_Ghaith.pdf

⁸ Vikram Babbar, “Trade-based money laundering—A macro view of the changing dynamics,” *Forensic Diaries: A Fraud Investigation and Dispute Services Blog*, May 27, 2016, <https://forensiciariesblog.ey.com/2016/05/27/trade-based-money-laundering-a-macro-view-of-the-changing-dynamics/>

HOW FINTECH IS CHANGING THE COMPLIANCE LANDSCAPE

Fintech is the integration of financial services and technology that has emerged in the 21st century as a new sector in financial services. It includes a broad spectrum of innovative companies that are generally startups founded with the purpose of disrupting traditional financial products and services. In the last several years, mobile payments, money transfers, loans, fundraising and even asset management sectors have contributed to the growth of Fintech. Companies such as PayPal, Kabbage, Lending Club, Square, Venmo and GoFundMe are recognizable brands that have fast become mainstream.

Citigroup reports that investment in Fintech has increased from \$1.8 billion in 2010 to \$19 billion in 2015.¹ Fueled by the rise of a mobile, on-demand economy and widespread public frustration with the banking industry, acceptance of these alternative services continues to grow, as evidenced by the impact that digital disruption is having on the financial industry. A recent article in the *Wall Street Journal* indicates that there are now more than 4,000 Fintech companies in the U.S. and U.K. alone.²

The battle between old and new

Legacy technology, slow deployment cycles for new technology and the inability to attract top technological talent are some of the challenges that banks face today if they wish to compete in the digital future. Regulatory and cost-reduction constraints are other factors that may cause these incumbents to lose out to new players who can deliver financial products and services more rapidly and efficiently. However, banks still have the advantage of an established customer base, capital and knowledge of compliance and regulatory requirements. When assessing the Fintech landscape, banks must have a clear digital strategy when deciding to compete, collaborate or buy.

Technology pundits have given banks three to five years to become digitally proficient or risk becoming a digital



laggard with declining profits. To succeed competitively, banks must invest in upgrading web and mobile technologies and adopt a Fintech culture that includes opening up application program interfaces, using agile development and even hosting hackathons to encourage collaboration.

A report published by the Economist Intelligence Unit titled “The Disruption of Banking,” indicates “there is a strong correlation between the strengths of banks and the weaknesses of Fintech, and, conversely the strengths of Fintech and the weaknesses of banks.”³ This correlation—combined with a common goal to deliver a seamless customer experience—has prompted partnerships that keep Fintech com-

panies agile and innovative and banks competitive in building excellence in technology and customer experience. One such example is the investment that Santander, Scotiabank and ING have made in Kabbage, an automated lending platform for small businesses. Kabbage offers loans in partnership with these organizations at a lower rate while reducing each bank’s back-office costs and making loan processing more efficient.

Whether the strategy is to go for it on their own or through a Fintech partnership or acquisition, digital innovation will allow banks to create value in several ways:

- Greater connectivity with customers, employees and suppliers

- Better decision-making due to improved data analytics
- More efficient automation and workflow with straight-through processing
- Ongoing product and business innovation

The changing compliance landscape

Consumers want easy access to save, spend and borrow money and will seek providers who best meet their needs. According to Javelin Strategy & Research, 126 million Americans will use mobile peer-to-peer payment apps by 2020, which represents a 50 percent

¹ Citi GPS: Global Perspectives and Solutions, “Digital Disruption: How Fintech is Forcing Banking to a Tipping Point,” March 2016, <https://www.citivelocity.com/citigps/ReportSeries.action?recordId=51>

² Rachel Witkowski, Telis Demos and Peter Rudegeair, “Traditional Banks Facing New Rivals,” *The Wall Street Journal*, December 4, 2016.

³ Economist Intelligence Unit, “The Disruption of Banking,” October 20, 2015, <https://www.eiuperspectives.economist.com/technology-innovation/disruption-banking>

BANKS AND REGULATORS HAVE LIMITED EXPERIENCE MANAGING NEW TECHNOLOGIES, ESPECIALLY THOSE THAT SERVE THE UNBANKED

increase from today.⁴ However, Fintech's disruption of the financial sector comes with new risks. Banks and regulators have limited experience managing new technologies, especially those that serve the unbanked. Regulators must balance the need for new technology that provides better services while controlling new operational risks brought about by the aggressive growth of unregulated financial services.

The regulatory uncertainty of non-bank financial services has caused gaps in consumer protection. Data security and transparency issues have been problematic for some popular peer-to-peer payment companies in the recent

past. While nonbanks may be subject to the same consumer protection laws as banks, they do not have the supervisory relationship with regulators.

U.K. regulators step up

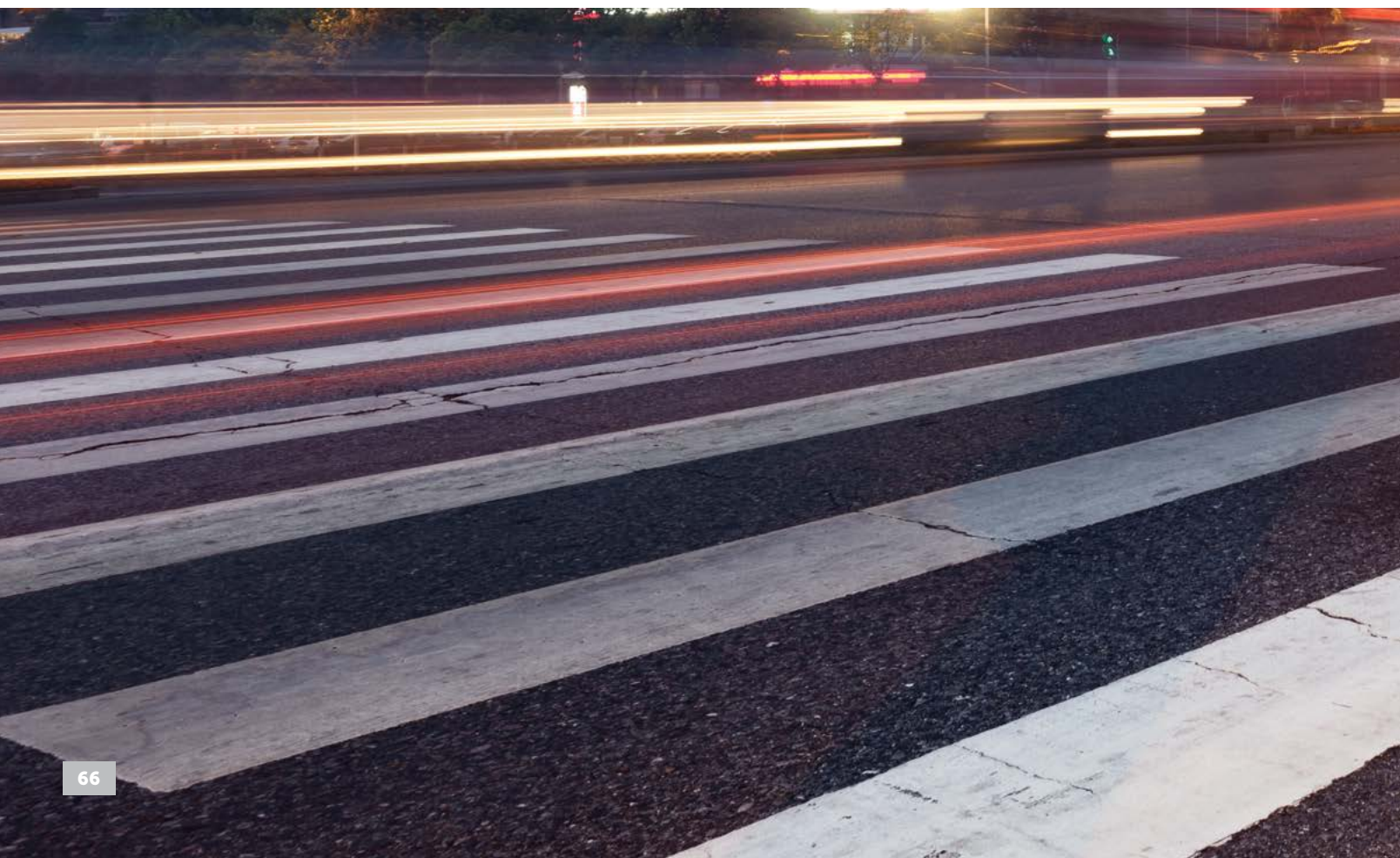
Recognizing the need for regulatory involvement in this new sector, the U.K. has been quick to action and leads the U.S. in this endeavor. In October 2014, the Financial Conduct Authority (FCA) initiated Project Innovate to promote competition in innovation to benefit consumers. A bank startup unit was created in January 2016 to help nonbanks determine if they should become banks and to educate these firms on regulatory requirements that they may be subject to under a bank charter. As part of Project Innovate, the FCA opened a regulatory sandbox in May 2016 where Fintech companies could test innovative products, services, business models and delivery mechanisms in a live environment while ensuring that consumers are appropriately protected.

The FCA was the first regulator to launch such a program. "In many ways it won't be just the firms that are learning in the sandbox. We will be, too," said Christopher Woolard, FCA director of strategy and competition, in his April 11, 2016 speech to the Innovate Finance Global Summit. Considered a unique but promising approach to managing new risks, regulators across the globe are closely monitoring the outcome of this experiment. The metrics are beginning to show that the U.K. government's proactive approach has created a very strong Fintech ecosystem generating 6.6 billion pounds in revenue in 2015 and employing 61,000 people. This has encouraged regulators around the world to explore this approach with some moving forward to adopt similar sandbox initiatives.

The U.S. takes action

On October 26, 2016, the Office of the Controller of the Currency (OCC) announced its decision to establish an Office of Innovation and implement a

⁴ John Engen, "Try to Catch Venmo in Person-to-Person Payments," *The American Banker*, January 9, 2017, <https://www.americanbanker.com/news/try-to-catch-venmo-in-person-to-person-payments>



framework supporting responsible innovation. The framework includes the creation of chief innovation officers (CINOs) in New York, San Francisco and Washington, D.C., to facilitate communications between the OCC and Fintech firms. The framework also promotes increased hiring of technical talent and has the potential to create a pilot program for testing new solutions and enhancing risk management before a committed roll out. Pilot programs would only be available to OCC-supervised banks and their Fintech partners with the stipulation that they must comply with all relevant consumer protection requirements.

In December 2016, the OCC went one step further when they announced that they would begin to grant limited purpose bank charters to Fintech companies. The OCC's authority to grant charters for national banks and federal savings associations also includes special purpose national banks. Limited purpose bank charters are granted to

trust banks and credit card banks and will now extend to Fintech companies engaged in bank-permissible, technology-based innovations in financial services. While Fintech companies—ranging from online lenders to virtual currency and payments companies—applaud this move, consumer advocates and state regulators cite concerns that the OCC will not follow through on its pledges to hold Fintech companies to the same standards of safety, soundness and fairness as other federally chartered institutions.

Capital requirements, state interest rate caps for lenders and community reinvestment requirements are some of the issues raised if the OCC opens up the federal banking system to Fintech companies. But, even before the announcement and despite the potential for more detailed federal scrutiny of business models, board structures and capital levels, some Fintech firms were seeking a national

charter citing benefits of reducing costs and increasing their ability to conduct business.

Regulatory risk is a major concern for companies developing innovative financial products and for those partnering with Fintech startups. While the U.K. and U.S. have taken different approaches to integrate Fintech firms into the compliance landscape, the common challenge is finding the right balance in regulatory oversight that allows Fintech firms to pursue innovation with confidence and certainty. Fintech companies are here to stay. The healthy cooperation of banks, regulators and Fintech firms will ensure better industry economics and customer experience while mitigating the risks introduced by new products. 

Carol Stabile, CAMS, senior business manager, Safe Banking Systems, Mineola, NY, USA, carol.stabile@safe-banking.com



ACAMS® | CHAPTERS



The ACAMS Chapter Development Program aims to focus the association's international efforts in anti-money laundering education and training at a local level. Chapters foster professional relationships and provide local forums for discussion around region-specific issues.

**Chapters launching soon*

Cultivating Comradery Worldwide



Find a local ACAMS chapter near you or start one today!

www.acams.org/chapters | chapters@acams.org

FINTECH: Two sides of the compliance coin

Fintech is a term that has entered the collective public consciousness in recent years. There is an increasing awareness of the disruption and exciting opportunities Fintech is bringing to financial services and consumers alike. This article looks at the benefits of Fintech, some of the challenges, and examines how the world of financial crime and Fintech complement each other. But, first, what exactly is Fintech?

Investopedia describes it as follows:

“Fintech is a portmanteau of financial technology that describes an emerging financial services sector in the 21st century. Originally, the term applied to technology applied to the back-end of established consumer and trade financial institutions. Since the end of the first decade of the 21st century, the term has expanded to include any technological innovation

in the financial sector, including innovations in financial literacy and education, retail banking, investment and even cryptocurrencies like bitcoin.”¹

Not only is Fintech bringing transparency and openness to the industry (take the foreign remittance services, which brings price transparency to users, or crowdfunding, which opens up access to funds for firms that might otherwise be excluded from traditional bank funding), but it is also helping to tackle financial exclusion.²

However, there are risks associated with the rise of Fintech, as noted by the Financial Action Task Force (FATF): “The greatest risks of Fintech are often the lack of oversight or governance and the anonymity they can provide.”³ FATF provides sample case studies in its transcript of FATF’s Executive Secretary at the XXV International Financial Congress in St. Petersburg on July 1, 2016. All three cases focus on the use of Fintech in support of terrorist financing activity, whether via e-wallets, social networks or the use of Bitcoin. This risk is heightened in the context of the more globalized nature of illicit financial crime networks and money transfers, which—without the right controls in place—Fintech could unwittingly facilitate.

With that in mind, how are financial crime risk management, compliance and Fintech converging (or indeed diverging)? Let us look at the associated challenges and opportunities through the

eyes of a compliance officer at an established bank, aiming to onboard a new Fintech business customer:

After having completed the relevant identification and verification processes of the Fintech firm’s ownership, the officer would likely begin by reviewing the perceived risk elements of the relationship, and determine whether the risk profile sits within their organization’s risk appetite. This review could commence with developing an understanding of Fintech’s own approach to financial crime risk management and the culture surrounding this. Here are a range of concerns, rightly or wrongly, attributed to Fintech:

- How do the disruptive tendencies inherent in Fintech firms align with their ability to comply with relevant regulation, particularly in anti-money laundering, counter-terrorist financing and sanctions? For example, how do they apply financial crime risk analysis within rapid product development cycles that form part of their market differentiator and how do they channel their enthusiasm to challenge the status quo when it comes to the application of the letter, and more importantly, spirit of the regulations around KYC? Given that many disrupters (not necessarily in finance) have purposefully challenged existing regulation, how will these cultures work together to create an appropriately robust financial crime risk management approach?

¹ “Fintech,” Investopedia, accessed January 15, 2017, <http://www.investopedia.com/terms/f/fintech.asp>

² Hannah Gould, “What You Should Know About Fintech and its Positive Powers,” *Guardian*, February 3, 2015, <https://www.theguardian.com/sustainable-business/2015/feb/03/what-you-should-know-about-fintech-positive-powers-banking>

³ David Lewis, “Accessibility of Financial Services: Challenges and Opportunities for Development,” FATF, July 1, 2016, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-international-financial-congress-july-2016.html>



- In a similar vein, is there a risk that the customer journey is more important than building a compliant process?
- Given how new some of these firms are, do their staff have the right expertise in place to manage the complexity of financial crime and compliance?
- What do their policies, processes and procedures look like? Have they thought about risk appetite and how will they identify and mitigate risks? Do they provide staff training?
- Will their relationship with the regulator be positive, negative or indeed nonexistent? And how tested is the compliance technology that they are deploying?
- Finally, what does their customer base look like and where is most of their transactional (if relevant) activity conducted? Have they considered their overall risk profile and how that will be managed, particularly if it is international, as many offerings are?

These are the right questions that should be asked that could raise legitimate concerns if any of the areas are particularly deficient. However, it is worth considering that within these risk areas, there are also some opportunities:

- The disruptive tendencies previously mentioned could lead to significant improvements in the financial crime risk management space, helping to establish

frictionless and efficient onboarding, risk identification and investigation procedures, all supported by technology that might well be more advanced, or at least tailored to the business model, than the prevention and detection systems in place at more traditional organizations.

- Building a new business model from scratch will inherently bring a much more manageable set of data which is of far better quality and structure.
- Due to the nascent build out of Fintech firm's organizational structure and its product offering, there is a potential for financial crime risk management and compliance teams to play an important role in shaping both the surrounding governance and the product itself, ensuring that a smooth customer experience is balanced with appropriate and innovative risk controls.
- Although staff at a Fintech firm may be inexperienced, they are often very bright, with strong intellectual and/or design credentials. In many instances, they also have equity stakes in the business they work for, meaning there is a high motivation to ensure that the venture is a success. This can have positive impacts on the management of financial crime in the firm.
- Similarly, there is a real opportunity for compliance and financial crime teams to influence the build out of risk policies, processes

and procedures, ensuring they are actionable, intelligent and proportionate to the risks the Fintech firm faces, while also building global standards from the get-go.

- Furthermore, there is an opportunity for a Fintech firm to develop a positive relationship with the regulator from the outset, provided they are thinking carefully about financial crime risk management and compliance. A cooperative relationship here could give rise to exiting regulatory developments and bring benefits to new and legacy financial services.

Given the evolution of crime and its evermore global nature and desire to find new forms of value transfer, it is in everyone's interest to help prevent the ongoing development of crime, whether that is in a more established organization, or in a new one. As such, it is imperative that both elements work together through doing business with each other, collaborating on projects, offering funding or banking services, or through information sharing forums. There are of course some risks in doing business with the Fintech community, particularly as they are pushing the envelope on many fronts and are proud of their inherently disruptive nature; however, there are also risks in dealing with more established firms that might be slower to respond to change and less nimble in handling new financial crime typologies. In the end, there is a fantastic opportunity to learn from each other, while bringing customers better service, transparent and affordable pricing, while tackling financial crime and advancing inclusion. 

*Robert Evans, director,
FINTRAIL Ltd, London, U.K.,
robert.evans@fintrail.co.uk*

*Gemma Rogers, director,
FINTRAIL Ltd, London, U.K.,
gemma.rogers@fintrail.co.uk*

TOP TALENT: FINDERS KEEPERS



As the world moves to an increasingly automated and technologically advanced environment, the best and most sophisticated systems will not improve efficiency if the people using those systems have inadequate skills, knowledge, or experience. Highly effective and well-trained anti-money laundering (AML) professionals who can apply their experience and honed skills can utilize technology to the maximum extent to increase efficiency and produce the best results.

Finding and retaining qualified team members in an exclusive community is a challenge for organizations that support the AML mission. The AML community typically consists of professionals who are familiar with the mission, such as law enforcement or individuals who have worked their way through the banking system into AML and respective to the U.S.' Bank Secrecy Act (BSA) compliance. This leaves many organizations asking how they can recruit fresh talent, perhaps even from outside the community. In addition, financial institutions have to focus their recruitment efforts on Millennials, equating to a change in the financial organization environment. Millennials look for meaning and purpose in their careers, which is not a major contrast to previous generations, but a solid mission with clear direction is requisite if we want to recruit and retain the best and brightest.

This article serves as a road map for recruiting and retaining top AML talent as it relates to the development of entry-level to mid-level positions.

The interview: Finding the ideal candidate

The interview process is pivotal when selecting your next AML superstar; thus, it is important to ask quality interview questions. The goal of the hiring manager or interviewer is to ask the right questions to identify talent that best fits the position. The interviewer should focus on the immediate and future needs of both the AML program and the institution. Preparing targeted interview questions that demand interviewees to think outside the box will help identify the best candidates.

Every interviewer has their standard interview questions that most of us are familiar with and typically ask in some variation, for example:

1. Why do you want this job?
2. What do you find meaningful about the financial crimes industry?

3. Describe what you expect from the day-to-day work in this position?
4. What would you like to be doing in five years?

However, these are surface level questions. Conducting a targeted interview will identify the depth of knowledge and skills the candidate will bring to your AML program. This approach provides the hiring manager with a solid understanding of the strengths and weaknesses, core skillset, requisite training, and most importantly how to properly lead the candidate going

**THE GOAL OF THE HIRING
MANAGER OR INTERVIEWER
IS TO ASK THE RIGHT QUESTIONS
TO IDENTIFY TALENT THAT
BEST FITS THE POSITION**

forward. At this point, it is imperative to determine if the candidate has the ability to convey or learn the skills needed to be an effective AML professional within your program.

The interviewer must be flexible when candidates offer experience from previous non-investigative or AML-related positions. At the entry-level or mid-level, the candidate may or may not have previous experience in a similar field; thus, it is important to be aware of the risk associated with inflated experience outside of the industry. However, the combination of their education, experience, skills and personality should shine through and give a solid indication of their ability to learn and ultimately prosper in the role.

Consider using the targeted questions or scenarios found on page 74, depending on experience, during the interview.

The answers to these questions will begin to show the candidate's attention to detail, analytical skills, decision-making, written and oral communication styles, and strategic thinking ability. All other things considered, one of the most important questions is, "What about this position and industry motivates you and what motivates you to do a good job?" Understanding what drives an AML professional to their peak performance will better help you determine if the role is right for the candidate and if so, engineer a development plan that both motivates and retains the best team member for your AML program. As Stephen Covey stated, "If you can hire people whose passion intersects with the job, they won't require any supervision at all. They will manage themselves better than anyone could ever manage them. Their fire comes from within, not from without. Their motivation is internal, not external." That said, a passionate and qualified AML candidate may need little day-to-day management; however, they will require transformational leadership in order to execute higher levels of performance and satisfaction within their role.

Transformational leadership

Transformational leadership (TFL) is a process whereby a leader engages with others and creates a connection that raises the motivation and morality in both the leader and the team member.¹

Transformational leaders demonstrate several key behaviors:

- *Developing and communicating a clear vision:* Transformational leaders help their team members connect the "what" (the execution of daily tasks) with the "why" (the vision and strategy), so that subordinates have a greater sense of purpose and can understand the value of their individual efforts.

¹ TRIBUSALLEN, Transformational Leadership, Theoretical Summary and Practical Applications.

CANDIDATE WITH AML EXPERIENCE	CANDIDATE WITHOUT AML EXPERIENCE
Start to finish, walk me through how you would conduct a financial crimes investigation.	Provide an example when you had to present complex information in a simplified manner in order to explain it to someone.
What logical, reasoning and analytical steps do you go through to determine if alerted activity is or is not suspicious?	When there is too much work to be completed in one day, how do you prioritize your tasks?
Describe your process for documenting whether or not alerted/identified activity is suspicious?	What process do you use to clarify your written work and to verify its accuracy? Have you developed a precise routine to confirm its accuracy?
Describe the type of suspicious activity that you typically file suspicious activity reports (SARs) on (omitting all identifying information).	Describe an experience where you had to complete a project or a task with a fixed, pressurized deadline, where the final delivery had to be near flawless.
What are the top five information components that should be included in a suspicious activity investigation and/or a high-risk customer review?	What is your approach for handling projects or tasks with a short deadline that require precise analysis, logic and calculations?
Specific to high-risk customer reviews, describe the process you would undertake to perform effective enhanced due diligence.	Tell me, as applicable, an assignment you worked on in which you had amassed a huge amount of data and then analyzed it to draw a conclusion.
In which areas within AML do you consider yourself a specialist, and in which specific areas do you need to expand your knowledge to become more proficient at this job?	Describe a situation or task that really tested your analytical abilities.
Describe a situation where you could not determine whether the activity was suspicious or not on your own. What steps did you go through to draw the final conclusion?	How would you manage a situation where you believed that something was not in compliance with professional, regulatory or ethical standards? Have you ever faced such a situation? If so, please describe.
Describe your previous responsibilities and daily/weekly workload metrics (e.g., number of investigations, alerts, high-risk customer reviews, OFAC dispositions, etc.) at your previous job.	How do you react in a situation where you need to make an immediate decision? What process will you follow for decision-making in a critical situation?
Why should we choose you over the other candidates? What skills, qualifications and experience make you the ideal candidate?	Why should we choose you over a candidate with experience? What skills, qualifications and experience make you the ideal candidate?

- *Using unconventional strategies/forms of influence:* Transformational leaders do not rely solely or heavily on formal rank/position or legitimate authority in order to influence their team. Instead, they rely on their own competence and the strength of their relationships with team members as primary power bases and use tactics that elicit more than just subordinate compliance.
- *Communicating high expectations of, and confidence in followers:* Transformational leaders know that belief in one's personal ability (self-efficacy) is a key factor in accomplishing a task, so they help boost the self-confidence of their subordinates. Not through fluffy compliments, but rather through relevant training and sufficient resources and by referencing the skills and abilities they know their subordinates possess.
- *Showing individualized concern for followers:* Transformational leaders work to establish supportive climates in which they listen carefully and tend to the needs of their team. They act as coaches and advisors while developing subordinates by delegating tasks and providing challenging experiences. Transformational leaders get to know their people (their strengths, weaknesses, goals, etc.), so that they can tailor their leadership approach to the unique individual.
- *Demonstrating self-sacrifice:* Transformational leaders are committed to a cause greater than self. They place the needs of their team and the organizational mission ahead of personal gain and well-being.
- *Acting confident and optimistic:* Transformational leaders understand the concept of emotional contagion where individuals throughout an organization often adopt the mood of the leader. Therefore, they exhibit a positive spirit and work to infect those around them with it.

- *Using emotional appeals:* Transformational leaders exhibit a high degree of emotional intelligence and are adept at stirring the emotions of their team in order to motivate them to work toward the organization's envisioned future.²

Through transformational leadership, leaders, managers and mentors must develop a thriving environment, so that their AML professionals can understand their purpose and value to the AML program and in addition, develop goals and a career path where they can continue to mature their skills and knowledge.

Purpose and value

Most team members want to know “their work has meaning—that it helps someone else or makes the world a better place. When people understand the deeper purpose behind their work, they are likely to be more satisfied and more productive.”³ As a leader in the AML industry, communicating the meaning behind AML professionals' work can be a somewhat easy task. An exercise to demonstrate the purpose and value in their work would be to provide insight on how an individual alert through the suspicious activity monitoring program, investigation, SAR filing, currency transaction report filing may play a larger part in providing law enforcement key information in combating financial crimes, human trafficking and terrorist financing. An alternative approach to consider: address high-profile world events or catastrophes and speak to how their job responsibilities may play a part in preventing a future occurrence. For example, the 9/11 Commission released a monograph that detailed how the 9/11 hijackers received money from wire transfers, cash and traveler's checks, and credit or debit cards for overseas bank accounts.⁴ The leader should speak to the financial component of the terrorist attack and provide insight on how their purpose within the AML program is to review, identify and report

suspicious transactions that may assist in preventing another terrorist attack. Demonstrate self-sacrifice and passion during these training opportunities.

Team members also need to feel valued and appreciated. If they do not, your high performing team members will pursue other opportunities. Through training, learning and professional development opportunities, a team member will see you are investing in their talent. This is especially important when developing Millennials. “Millennials are concerned with investing their energy and their time in organizations that will reciprocate. They want to make sure they are growing inside their organizations and that they have a path to continue to do so.”⁵

Build career entrepreneurship

Establishing career entrepreneurship within your department promotes a culture of commitment, supported by strong accountability. Allow team members to set their career goals and understand their motivations and aspirations as their leader. Provide each team member with the tools to reach their goals and allow an avenue to measure their accomplishments. Assisting your team members to set their own career road map and then allowing them to succeed will ensure they remain engaged and loyal to your AML department and program. It is very important that both you as their leader and the team member know what really is their motivation. Working in an industry that motivates their core purpose, supported by a successful road map, will provide the team member with a sense of satisfaction and purpose.

Several other initiatives can be built within the AML career entrepreneurship initiative to ensure you are addressing development plans and career paths that include:

- Short- and long-term goals and wins

² Ibid.

³ “Helping Your People Find Purpose in Their Work: Finding Deeper Meaning in a Job,” accessed January 23, 2017, <https://www.mindtools.com/pages/article/find-purpose-work.htm>

⁴ “National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing,” accessed January 23, 2017, https://9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf

⁵ Sharon Florentine, “Investing In Your Employees' Career Growth Drives Satisfaction,” CIO, July 4, 2016, <http://www.cio.com/article/3091035/it-skills-training/investing-in-your-employees-career-growth-drives-satisfaction.html>

- Personal reflection opportunities
- Effective feedback for both direct reports and peers
- Strengths and areas for development, including plans for visible performance improvements
- Development initiatives and performance metrics

Consideration may also be given to hosting periodic skip-level meetings. Skip-level meetings are an effective tool where the manager's manager (AML program leader) meets with team members to discuss concerns, obstacles and opportunities for improvement. The meetings should provide a strong focus on maintaining or improving overall communication by allowing different perspectives to be presented and shared and developing effective relationships. The point of this meeting is to listen and to ensure that the communication is freely flowing in both directions. This is an opportunity for leaders to listen to the real talent within their department, entry- and mid-level experts. If leaders are unwilling to listen to their team, this can create a devastating disconnect that could derail the mission or encourage turnover of your top AML talent.

Examples of topics to be discussed in skip-level meetings with team members:

- What is or is not working well in the department right now? The risk of asking this is assumed by the manager or leader to determine inflated versus real issues. It is easy for leaders to fall into the mentality of hearing, but not listening.
- What is one thing we should start, stop or continue to do in order to be more successful?
- What, as a team member, do you need more or less of from your managers in order for you to be successful as a department and in your role?

It is essential for leaders to follow-up with department managers to discuss feedback and trends. This is the leader's

chance to guide managers on how to improve their team or management to find success.

Involving entry- to mid-level analysts into the enterprise-wide picture will provide a sense that the organization can only function with the input from the experts on the day-to-day activities, which is true. By showing your AML talent how important they are to you as their leader and your AML program, you will find your team more engaged and have more buy-in in the mission you are accomplishing. Although it must be clear to each level that it is because the leader seeks entry- and mid-level involvement that the AML program is successful, it is not necessarily the other way around.

Optimal performance

Strong talent is an asset to your organization. Use it. Ask and involve your top AML performers how to approach new and emerging challenges, large implementation efforts and special projects. If you have a top performer, ask him/her how to approach a project, challenge, etc. For example, many within the financial industry are challenged with the implementation of beneficial ownership. Spearhead a mind or process mapping meeting with your talented AML team or top team member on steps and initiatives they would recommend to implement a regulatory requirement. This will provide an opportunity for innovation and transparency supported by an environment where your team is engaged and will have greater buy-in of any supplemental tasks and projects that may evolve as a result of the initiatives addressed.

The opinions and recommendations provided by your talent will continue to improve the more experience and training they receive. Cross-training is a great way for you as their leader to recognize those employees who are imperative to your AML program. In addition, it provides insight on your AML professionals who are ready to take on added responsibility while providing an avenue of growth for learning more about the organization or more

specifically the AML program and industry. Your talent can teach others in your organization or department and it can even positively impact efficiency within your AML program.

Conversely, if your talent is siloed into one specific area within your AML program, you may not visibly be able to see or know areas of additional strengths where they may bring measurable value. Implementing a cross-training program properly will yield successful results, both for the leader and the AML professional. Specific to the AML industry, implementing the Icebergs Competency Exercise (ICE)⁶ as part of your cross-training program will provide an avenue of growth and development of a talented AML team-member.

Icebergs Competency Exercise (ICE)

The Icebergs Competency Exercise⁷ tool can be used as part of training initiatives and the development of AML teams. As shown in Figure 1, an iceberg is 10 percent ice above water, while the other 90 percent of it remains underwater. As a leader, take a moment to reflect on your team to determine how much talent you are actually using. This could lead to adjusting roles, applying additional training or other actions; however, the purpose of the ICE is to cross-train and introduces the larger picture of the AML mission into individual team members. This is essential if an organization wants to have a successful team and AML program that can achieve meaningful goals. The ICE program was created to promote development, increase efficiency, improve processes, respond to fluctuating workflows and to provide an avenue for AML professionals to see the big picture. On the other hand, this requires the organization to make time for managers to analyze their teams. So often, our managers become focused on daily tasks that can overwhelm their purpose. Leaders can designate analysis sessions for managers to maximize team efficiency.

⁶ Lauren Kohr, Icebergs Competency Exercise, AML/BSA Cross-Training Approach, 2016 ACAMS AML Professional of the Year, Senior Manager, Financial Intelligence Unit, Pentagon Federal Credit Union, January 2017.

⁷ Ibid.

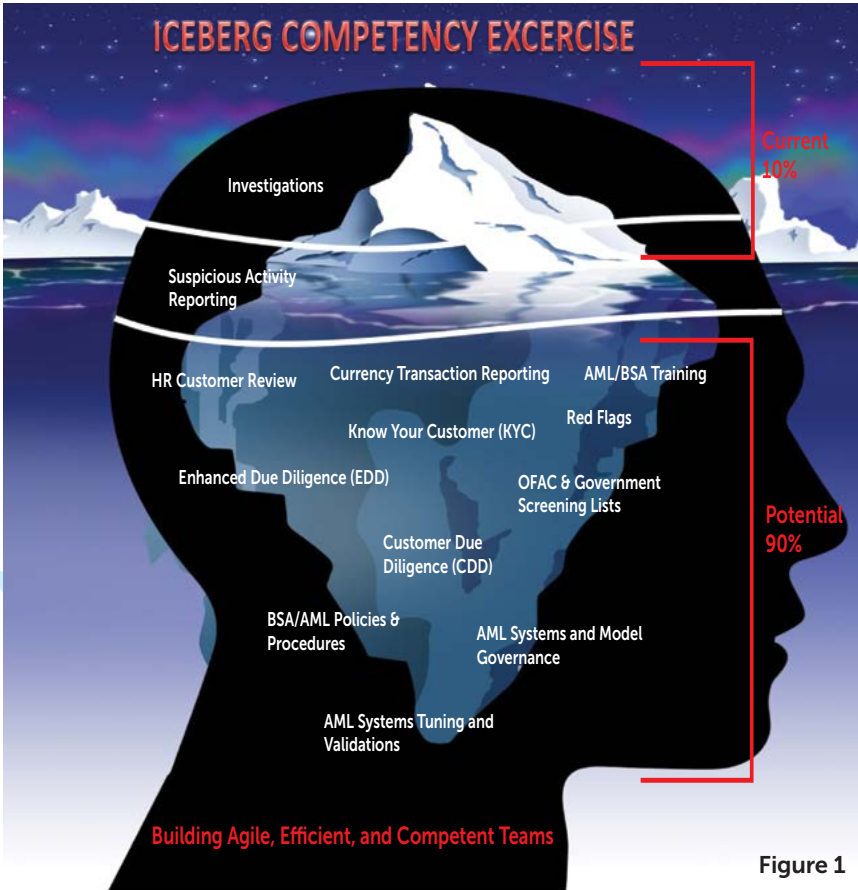


Figure 1

Key takeaways

When it comes to hiring and retaining top talent within the AML industry, the key takeaways are:

- Prepare targeted interview questions that demand interviewees to think outside the box and allow you to identify their skill and knowledge set
- Demonstrate transformation leadership through the seven key behaviors
- Establish career entrepreneurship within your department and AML program
- Ask and involve your top AML performers on how to approach new and emerging challenges, large implementation efforts and special projects
- Cross-training is a great way for your talent to grow by learning more about the AML program, industry, requirements and regulatory expectations
- Implement ICE as part of training initiatives and the development of AML teams

As a leader of your AML program you will be rewarded, not only with hiring and retaining talent, but also with loyal team members who contribute to both your AML program and organization's success.

Lauren Kohr, CAMS-FCI, senior manager of governance, risk and quality control, Pentagon Federal Credit Union, Alexandria, VA, USA, lauren.kohr@penfed.org

Zach Miller, CAMS-FCI, vice president and BSA officer, Mid Penn Bank, Harrisburg, PA, USA, zachary.miller@midpennbank.com

Implementing ICE throughout your training programs and career development plans is fairly simple. Each letter of the word “icebergs” is tied to a typical requirement or responsibility within an AML and BSA compliance program. Depending on the size and complexity of your institution, you may have silos within your program where team members hold specific responsibilities. Implementing ICE will allow the silos to increase collaboration and understand each other’s abilities and goals. The aim of this is to strengthen the team, more efficiently share information and improve skills across the board.

Investigations and Suspicious Activity Identification and Reporting

Currency Transaction Reporting and Exempt Entity Review

Enhanced Due Diligence (EDD), Customer Due Diligence (CDD) and Know Your Customer (KYC)

Bank Secrecy Act policy, procedures, risk assessment and training program

Examination Management, Audit, and QC/Program testing

Red Flags, Cyber Security, and Other Complex and Emerging Financial Crimes

Government screening lists

Systems and model governance, tuning and validation

ICE is also an opportunity for team members to identify different areas within AML compliance in which they are interested. Managers can guide team members into areas that could assist in gaining skills and knowledge that benefit both the individual and the organization. Use their interests to create development plans and a strategy for their future career within your organization.

MARKETING 101:

How an AML professional can increase marketability

The anti-money laundering (AML), counter-terrorist financing (CTF) and anti-financial crimes industry is booming. The evolving regulatory landscape, technological advances and new schemes create an environment where experienced industry compliance professionals are in demand. In this case, the demand is creating its own supply. New professionals enter the job market daily. So, how do you, as a seasoned AML compliance professional, best position yourself to not only remain employable today, but to advance in the industry tomorrow? The answer is marketability.

“Marketability...refers to how desirable a candidate is for employment consideration...Corporate employers...prefer to hire academically prepared, highly motivated and ambitious workers who offer them a good, long-term return on their investment. Marketability also denotes the flexibility a candidate enjoys in selecting suitable employment opportunities. That is to say, a highly marketable job seeker...can follow a number of different pathways to career success.”¹ To become marketable, demonstrate subject-matter knowledge and ambition. To remain marketable, share subject-matter knowledge and encourage ambition.

¹ Calvin Bruce, “How to Make Yourself More Marketable,” Experience, https://www.experience.com/alumnus/article?channel_id=careers&source_page=breaking_in&article_id=article_1139411761637

Learning the basics

It may seem intuitive, but one way to improve marketability is to expand subject-matter knowledge and skill-sets. AML and anti-financial crimes compliance is a vast industry comprised of lawmakers, regulatory enforcement officials, law enforcement, compliance professionals, technology experts, attorneys and more; therefore, understanding all the moving pieces can be a daunting proposition. Start with the basics—for U.S.-based professionals, read and understand the requirements outlined in the Bank Secrecy Act² (BSA) (for non-U.S. based professionals, substitute local regulations). Investing valuable time in understanding regulatory requirements is one way to differentiate oneself in the industry.

Remember to seek out and leverage other relevant and trustworthy

resources during the education process, such as supplemental industry websites (e.g., FinCEN, OFAC, etc.). While you are reading the requirements, create some useful and proprietary tools for yourself, such as 1) a requirements matrix, which can be readily converted to a control assessment, and 2) a resource guide, which can be leveraged as you progress in your career (more on this later).

Once the regulatory requirements have been mastered, U.S.-based professionals should move on to the Federal Financial Institutions Council BSA/AML Examination Manual³ to understand compliance expectations. Also, to help master the implementation and maintenance of a quality risk-based anti-financial crimes compliance program, read and understand the risk management integrated framework principles (aka Three Lines of Defense) put forth by the Committee of Sponsoring Organizations of the Treadway Commission.⁴

Remember the regulatory matrix you created when reading the BSA? Well, now you should be well prepared to add controls your institution has implemented—resulting in a very handy controls assessment document.

Seek out a mentor

Developing formal or informal mentoring relationships can reap multiple benefits:

Internal networking—Being seen with a more senior professional inside of your organization increases your profile among other senior managers.

External networking—“A well-connected mentor likely has inroads into influential professional organizations...perhaps a mentor can sponsor your membership in one or more of the prestigious organizations. The contacts

that you make through such associations can prove helpful throughout your career development. Plus, listing these associations on your resume will enhance your written credentials and give you a bit of a competitive edge in job hunting.”⁵

Proactively request not only of your mentor(s), but also of your manager to be a silent participant on relevant teleconferences and ask that appropriate referential material and/or emails be forwarded to you. This will provide exposure to 1) identify who is who in the corporate structure, 2) study appropriate interactions with varying levels within the organization and 3) learn new information, jargon, risks or processes.

Become the “go-to” person

The “go-to” person has many attributes—he/she always delivers a quality product on time and makes himself/herself available for extra assignments/work. Thus, when management asks for volunteers for an assignment and you feel qualified to tackle, be the first to raise your hand. When management approaches you with an assignment, enthusiastically accept it. Do not publicly complain to management or to peers about the added workload. Lead by example and take examples from your leaders. Leaders do not complain (publicly) about anything and neither should you. You want to be the person setting the bar for others, so act accordingly.

Proactively offer to provide written or oral summaries of white papers, interesting industry articles or enforcement actions. You may want to intentionally focus on areas outside of your current job responsibilities in order to grow knowledge and to demonstrate “fungibility” to management.

² “Electronic Code of Federal Regulations,” U.S. Government Publishing Office, January 1, 2017, http://www.ecfr.gov/cgi-bin/text-idx?SID=4ed28aff321d97007276a7736cae032e&c=ecfr&tpl=/ecfrbrowse/Title31/31cfrv3_02.tpl

³ “Bank Secrecy Act/Anti-Money Laundering Examination Manual,” FFIEC, 2014, https://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2014.pdf

⁴ Committee of Sponsoring Organizations of the Treadway Commission, <http://www.coso.org/guidance.htm>

⁵ Calvin Bruce, “How to Make Yourself More Marketable,” Experience, https://www.experience.com/alumnus/article?channel_id=careers&source_page=breaking_in&article_id=article_1139411761637

KEEP IN MIND THAT YOU ARE YOUR BRAND AND YOUR BRAND IS YOU

As you consider how to best represent yourself in front of management and peers, keep in mind that you are your brand and your brand is you. So, take very good care of both. Cleanse your online presence. Invest in a public speaking course or join Toastmasters International. Dress for success. Dress for the role you want and not the job you have.⁶ You are in the process of building your brand and appearance does matter.

By dressing for the job you want, you take the external and internalize it. Posture is straighter when dressed in a suit rather than casual attire. A professional attire will encourage professional interactions. Other people will more readily see in you the same potential for job growth that you see in yourself when you dress the part.

Taking knowledge to the next level

Building subject-matter expertise is a process⁷ that takes time and dedication. “Three elements are required to establish oneself as a subject-matter expert: education, experience and marketing. Having the right credentials fulfills the education component,”⁸ says Jesse Torres, community banker and small business expert. Many undergraduate schools offer studies in fields directly related to financial crimes prevention and analysis such as homeland security, criminal justice or forensic accounting. An undergraduate degree is not the only path into the industry. An advanced degree in law is appealing to many compliance-hiring managers. Perhaps more appealing than a law degree or law enforcement experience to AML compliance-hiring managers is having one or more industry certifications.

The value of an industry certification cannot be overstated. The compliance industry offers multiple certifications that may be useful in building subject-matter expertise such as a Certified Fraud Expert (CFE) designation and a Certified Regulatory Compliance Manager (CRCM) designation, but it is safe to say that the gold standard in anti-money laundering compliance remains the Certified Anti-Money Laundering Specialist (CAMS) designation offered by ACAMS. ACAMS now offers advanced certifications for those individuals who want to demonstrate commitment to a particular subject matter like audit or financial crimes investigations.

Find your passion

In building subject-matter expertise, it helps to find a passion and then study it and live it. Take your passion and strive to make a difference in your organization and/or in the industry. Within your organization, develop process efficiencies to eliminate waste, identify and/or control for gaps in the AML compliance program, offer education and training opportunities.

In the industry, share knowledge or develop new programs. ACAMS’ 2016 *Professional of the Year* award winner Lauren Kohr says, “This is what I am most passionate about: breaking down the traditional silos that have previously divided government, law enforcement, and the financial industry and replace it with relationships working collectively to accomplish our shared visions of combating financial crime. Such partnerships will promote the sharing of industry knowledge and best practices, as well as cross-industry dialogue aimed at preventing further growth of crimes aided through illicit financial transactions.” Kohr turned that passion not only into the 2016 *Professional of the Year Award*, but also the 2016 *ACAMS Today Article of the Year Award* by sharing her knowledge in an article titled “The Power of Peer Groups for Community Banks.”

Encourage knowledge sharing

Not only should you share your knowledge with peers and management, but you should also encourage others to share knowledge. Compliance programs become stronger when appropriate information is shared. In addition, remember, training is one of the five AML program pillars.

In her *ACAMS Today* article titled “Train Like a Champion,”⁹ Yashica Whitehead states “Knowledge is free. Employees can share what they know with other AML professionals within the institution. Providing a knowledge-based forum for employees encourages an open exchange of questions and ideas among AML professionals that enhances overall regulatory and best practice knowledge. It also promotes

⁶ R. Kay Green, “Dress for the Career You Want, Not the One You Have,” *Huffington Post*, January 31, 2013, http://www.huffingtonpost.com/r-kay-green/career-future-advice_b_2583884.html

⁷ Matt Cooper, “5 Steps to Becoming More Marketable,” *Inc.*, September 4, 2013, <http://www.inc.com/matt-cooper/5-steps-to-becoming-more-marketable.html>

⁸ Jesse Torres, “5 Steps to Becoming a Subject Matter Expert,” April 21, 2014, <https://www.linkedin.com/pulse/20140421082247-6260457-sell-more-become-a-subject-matter-expert-in-five-steps>

⁹ Yashica Whitehead, “Train Like a Champion,” *ACAMS Today*, March-May 2010, http://www.acamstoday.org/wp-content/uploads/2015/05/AT_v9_n2.pdf

continued knowledge sharing outside of the training environment by providing networking opportunities.” You can be the catalyst to develop the knowledge sharing forum in your organization. Seek out management support and you are on your way to increasing your profile and helping your organization. It is a win-win situation.

From a marketability standpoint, there is real value in sharing your own knowledge with others—your visibility within the organization and industry is automatically magnified. You will cement your role as a subject-matter expert by being the go-to person for answers to BSA/AML-related questions. What is the best way to share your knowledge? The opportunities are endless:

Internal to your organization:

- Create helpful tools and resources. When learning about a topic, bookmark links to share with managers and peers. Document the regulatory requirements in a requirements matrix and keep the matrix updated. Create a resource containing regulatory requirements, procedures, helpful bookmarks, samples of communications and calendars for new associates to leverage.
- Put knowledge to use by identifying compliance gaps in the program and offering potential solutions.
- Volunteer to put your skills to use—assist with risk assessments, systems testing, data validation or conduct line of business training.

External to your organization:

- Offer to speak at a local or national conference or teleconference (remember to obtain approval from within your organization, as needed). Expand beyond the AML/financial crimes boundaries. For

PROACTIVELY SEEK NEW RESPONSIBILITIES

example, accountant and attorney groups also look for industry professionals to speak at their meetings.

- Write an article or a blog (remember to obtain approval from within your organization, as needed). *ACAMS Today* and *ACAMSToday.org* welcome the written insights of industry professionals. Contact any Editorial Committee member or the editor-in-chief¹⁰ for additional information on article submissions. You have a unique viewpoint and unique experiences—share them.
- Volunteer to assist with your local ACAMS chapter. Proactively seek new responsibilities. A simple offer to volunteer may eventually develop into a leadership position within the organization.
- Create or join a peer group. As Kohr states in her award-winning article, “The benefits of a peer group become immeasurable, not only to BSA/AML representatives in the community banking industry, but to law enforcement, regulatory agencies and BSA/AML consultants. Each member—no matter the background or discipline

represented—is provided the opportunity to collaborate, share knowledge and experiences, network, and understand the challenges each discipline faces.” The exposure to like-minded professionals tackling compliance challenges is priceless.

- Network—and then network some more. When networking, ensure to hand out business cards. If your organization does not supply you with business cards, pay to have them made. It will be one of the best \$10 investments you will ever make! The value of a business card cannot be overstated when networking. Attend ACAMS chapter meetings and trainings. When possible, attend or present at national conferences. Remember to have a “30 second elevator pitch”¹¹ ready!
- Finally, remember to keep your resume and online presence updated with new skills, articles published or presentations delivered. “Given how competitive the job market is, a well-constructed resume is one sure-fire way to rise to the top of the applicant pool,”¹² states a recent *ACAMS Today* article. Richard Phillips, owner of Advantage Career Solutions stresses that professionals should maintain a smart online profile by removing inane or offensive posts and begin to contribute to industry blogs and forums.¹³

Becoming marketable in today’s job market takes time and patience. Staying marketable takes dedication and passion. Both results are worth the effort expended. **A**

*Amy Wotapka, CAMS, BSA manager,
Northwest Bank, Warren, PA, USA,
dascwotapka@verizon.net*

¹⁰ Found on *ACAMSToday.org*

¹¹ “The 30 Second Elevator Speech,” <http://sfp.ucdavis.edu/files/163926.pdf>

¹² Amy Wotapka, “Resume Tips for the AML Professional,” *ACAMS Today*, December 2016-February 2017, <http://www.acamstoday.org/resume-tips-for-the-aml-professional/>

¹³ Margaret Steen, “Eight Ways to Make Yourself More Marketable,” *Monster*, <https://www.monster.com/career-advice/article/8-ways-to-make-yourself-more-marketable-hot-jobs>

FOURTH TIME'S THE CHARM?

In December 2016, the Financial Action Task Force (FATF) issued its Fourth Round Mutual Evaluation Report for the U.S.' anti-money laundering and counter-terrorist financing (AML/CTF) measures. It weighs in at 14 pages of executive summary, 161 pages of the main report and 80 pages of annexes (including a glossary of acronyms used in the text that spans over three full pages). What could justify so much ink?

The Report is encyclopedic in nature, listing and explaining every governmental department, agency and task force, as well as each initiative and responsibility for each of the seven areas for which the U.S.' readiness and ability to combat money laundering and terrorist financing has been evaluated. Each of the evaluative chapters are preceded by a summary of findings and recommendations before they are explained in exhaustive detail.

The U.S.' AML/CTF capabilities were evaluated, most notably in the annexes, against FATF's Recommendations and evaluation criteria. A similar grading was last performed in the third round

evaluation in 2006. However, the criteria have changed since then due to the updates made to FATF Recommendations since that time, making the fourth evaluation less than straightforward when evaluating progress or lack thereof when compared to previous ones.

The good

The Report notes that the U.S. has a robust AML/CTF framework and that cooperation and coordination among law enforcement and government agencies has further matured since the 2006 Third Round evaluation. In addition, the financial sector understands its regulatory burdens and risks, and they have evolved their systems, policies and procedures accordingly.

Law enforcement agencies aggressively investigate and prosecute AML/CTF cases, and have a broad range of resources to conduct effective investigations. These translate to over 1,200 convictions annually. The Report also notes that the U.S. is working to improve the speed of responding to international mutual legal assistance and extradition requests.

The Report notes the effective use of asset confiscation, both criminally and civilly, including the use of civil forfeiture in some individual states. In a similar fashion, the U.S. was recognized for its success in blocking assets as part of the financial sanctions regulation.

Finally, the Report lauds the U.S.' oversight and enforcement of the banking and brokerage industries. In addition, it notes the improvement of that supervision in the money services business (MSB) sector, which has been achieved through coordination with state agencies. The available formal and informal enforcement measures "seem to have the desired impact on achieving the supervisory objectives."

The bad

The following were noted as areas where the U.S. could improve its adherence to FATF standards:

Designated non-financial business professions (DNFBPs)

AML/CTF requirements for DNFBPs, other than casinos and dealers in precious stones and metals, were noted as being significantly less rigorous than the published standard. The Report listed investment advisers (other than those working for a firm already subject to fuller program requirements), real estate agents, accountants, lawyers, trust company service providers and corporate formation agents as requiring more stringent standards based on their facilitation roles in situations that can be abused in money laundering or terrorist financing schemes.

However, as a practical matter, such requirements are unenforceable, other than at a significant expense. The report notes that there are about 1 million lawyers, approximately 1.2 million accountants and auditors, almost 400,000 real estate agents and over 360,000 investment advisers in the U.S. This is in contrast to the 13,000 banks, 4,100 broker-dealers, 900 life insurance firms and about 42,000 MSBs currently subject to more stringent requirements. Further complicating the issue is the fact that there are an unknown number of trustees, due to the lack of registration. Barring effective supervision of these professionals and enforcement of the corresponding violations, imposing AML/CTF requirements seem more of a box-checking exercise than actually reducing the risk of these crimes.

Beneficial ownership information

The report notes that being able to identify the beneficial owners of legal structures in a timely fashion contributes

LAW ENFORCEMENT AGENCIES
AGGRESSIVELY INVESTIGATE
AND PROSECUTE AML/CTF CASES,
AND HAVE A BROAD RANGE OF
RESOURCES TO CONDUCT
EFFECTIVE INVESTIGATIONS

INSTITUTIONAL
RISK

EMERGING
TRENDS

FUNDING
FLOWS

THREAT
ENVIRONMENT



significantly to AML efforts and that the lack of a regulatory requirement to collect such information in the U.S. was one of the most notable gaps in the U.S.' AML/CTF regime. An interesting comment made in the Report was that not only did this affect domestic oversight and enforcement efforts, but that it also impacted the ability to cooperate with international requests for assistance in investigations and prosecutions. When such information is not readily available, law enforcement agencies are pressed into service to identify the ultimate beneficial owners.

It should be noted that the evaluation documented in the Report was performed prior to the Financial Crimes Enforcement Network's (FinCEN) finalization of the Customer Due Diligence (CDD) Rule in July 2016, which requires the identification of beneficial owners by banks, securities brokers and dealers, futures commission merchants, and introducing brokers in commodities transactions.

THE REVIEWERS
RECOMMEND A
"FOCUSED RISK
REVIEW" OF THE
EXISTING THRESHOLDS

Other shortcomings of the U.S. program

Four other areas for improvement were noted in the Report:

State regulation and enforcement

First, the reviewers found limited information on state-level regulation and enforcement and no apparent sense of cohesion or uniformity between those states that had available information. To the reviewer, state programs should adhere to the same standards as the federal program and should be consistent to take away any "safe havens" from regulation and enforcement.

However, such assumptions neglect the jurisdictional separation between federal and state powers. Also, given that money laundering is a federal offense, any regulation or enforcement at any other level of government is a nicety that adds additional resources to the fight against financial crime, but not a necessity.

Reporting thresholds

The Report notes that the suspicious reporting thresholds in the U.S. (\$5,000 for banks and \$2,000 for MSBs) are not in line with the FATF Standards. For example, the Interpretive Note for Recommendation 20 notes that all suspicious transactions are to be reported "regardless of the amount of the transaction." The reviewers recommend a "focused risk review" of the existing thresholds.

This appears to be another case of where theory meets practice, and practice wins. While, in theory, any transaction can be suspicious, surveilling all transactions is impractical, given the size of the U.S. economy, the diversity and mobility of its population, the number of transactions by its citizenry and the razor-thin margins that industries like the banking sector operate under. If anything, a case could be made for raising those limits, as the

values originally established have undoubtedly increased when inflation is factored in.

U.N. sanctions

Secondly, the Report notes that the U.S. has not implemented all sanctions designations made by the U.N., and others have not been designated "without delay," as per U.N. resolutions. However, it does acknowledge that some of the gap is due to designations that do not have significant details to aid in the identification of the sanctioned party. They note that adding these lower-quality designations "would reduce the effectiveness of the system by generating an enormous number of matches" for which there would be no practical way to positively establish a match or non-match to a reasonable likelihood. The reviewers also considered whether or not, given the U.S.' banking volumes, processing bottlenecks might develop from these additional unresolvable cases and if they would have a significant negative impact on the global financial system. In addition, the reviewers' note that the effect of the missing designations has been minor, makes one wonder how that can be effectively measured.

Tax crimes

Finally, the reviewers noted that the U.S.' AML/CTF regime would benefit from the addition of tax crimes to the list of predicate offenses. The Report does mention, to its credit, that tax fraud (focused on income tax return

THE REVIEWERS NOTED THAT
THE U.S.' AML/CTF REGIME
WOULD BENEFIT FROM THE
ADDITION OF TAX CRIMES TO
THE LIST OF PREDICATE OFFENSES



fraud) is covered as a predicate offense under an umbrella fraud predicate in the 2015 National Money Laundering Risk Assessment. In addition, the reviewers did not provide a list of tax crimes that might be added as predicate crimes. However, in the past FATF has mentioned tax evasion as a predicate offense.

The ugly

The Report, while it is “logically” organized, is not effectively organized in order to highlight areas of improvement. There are eight chapters to the Report, as well as a technical annex that maps the gathered information to each evaluation criterion and provides a score for each FATF recommendation of Compliant (C), Largely Compliant (LC), Partially Compliant (PC) or Non-Compliant (NC). Each chapter is organized encyclopedically, which causes background information, improvement since the last Report and identified gaps to be grouped together because of their common materiality to the sections, rather than separated by their value in understanding the material. This results in the same deficiencies being called out over and over again in different sections of the same chapter, not to mention different ones, which may be less effective to making the deficiencies and their overall impact clear than listing the deficiency once and explaining all the implications. For example, the term DNFBP appeared on 79 pages of a 264 page document, including every chapter of the Report except for the one focused on international cooperation.

A recommendation for FATF would be to consider reorganizing the information in the Report to make it more action-oriented in achieving its goals of better AML and sanctions compliance. For example, it might be better to organize each chapter into separate sections for documentation of the current program elements, the improve-

ments since the last report and the notable gaps. Then, a chapter devoted to the gaps across all sections, and the related recommended action steps, could be added to provide a single place to understand the totality of the compliance regime.

In addition, the Report could be more reader-friendly if it could reduce its dependence on acronyms. Having a glossary for such a lengthy, complex document should be for the purposes of gathering all such acronyms in one place, and not as a place for readers to refer to when reading the document. If the acronyms were more or less strictly alternated with the complete name throughout the body of the text, it would make the report more readable for the less expert, as well as for the more attention or time-starved.

The verdict

Ultimately, the U.S.’ AML/CTF regime, which has improved from the 2006 Report, was left in FATF’s regular follow-up process, which is the norm for members without significant program deficiencies. The Report specifically calls out the U.S. for not addressing shortcomings in meeting Recommendation 5 from the 2003 Recommendations, which focuses on CDD. While not explicitly mentioned, it is not unreasonable to infer that this was specifically because the AML/CTF regulation (at the time of the evaluation in early 2016) did not require the identification of beneficial ownership information. Given the advent of FinCEN’s new CDD Rule, one should reasonably expect higher ratings the next time around.

However, as there is no outcome that is less rigorous or less frequent than a regular follow-up, according to FATF’s documentation regarding the Fourth Round, the U.S. has no real incentive to improve the quality of its regulatory regime. If there were a mechanism to go on a longer review cycle, or one to focus only on specific gaps, rather than a complete program review, it might provide an appropriate impetus to close the remaining deficiencies.

The Fourth Round Mutual Evaluation Report of the U.S. is, indeed, comprehensive and encyclopedic, documenting the efforts to combat financial crime in expansive detail. One wishing to have comprehensive knowledge of the lay of the land could do a lot worse than starting with this tome. However, its organization makes it more difficult to digest than it could be, as both a textbook to the U.S.’ AML/CTF efforts, and especially for having its analysis and recommendations clearly understood and acted upon. Hopefully, by the next review, FATF reviewers will find the secret ingredient to producing a report that both comprehensively documents its findings and produces a leave-behind that is actionable. **A**

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

The views in this article are those of the author and do not necessarily represent those of ACAMS or any of its affiliates.

2017

TRANSITION AND TRANSFORMATION FOR EUROPE

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

As we move through the first months of 2017, the long-awaited 'big day' for the EU Fourth AML Directive has arrived, the Fifth AML Directive is under discussion, and I wonder how prepared you feel to manage the myriad and complex changes at work.

The scale of transformation and transition facing our community will be the key theme at the *ACAMS 13th AML and Financial Crime Conference* on June 1-2, 2017, in London. Also for the first time, in response to member requests, we will be running a workshop dedicated to mastering the skills required to introduce and incorporate change into your anti-financial crime compliance programs.

As ACAMS membership and chapter networks expand across Europe, I am delighted to let you know that we are now able to offer you European business hour support in English, French, Portuguese, Russian and Spanish (we will soon be adding German). In addition, the CAMS sixth edition will be available in all these languages shortly.

Finally, here is an update on upcoming training events in Europe through June 2017:

- *ACAMS Anti-Financial Crime Symposium:* Okura Hotel, Amsterdam, Tuesday, March 7

- *CAMS Examination Prep Seminar:* Hellenic Banking Institute, Athens, March 16-17
- *Fintech, Crowdfunding and Other Innovative Businesses: Avoiding Trying to Force Square Pegs in Round Holes:* Friday, April 21, 2017 12:00 PM – 1:00 PM BST, Free Webinar
- *Second and Third Line of Defense Activities: Designing an Effective Anti-Financial Crime Review Program: ACAMS 13th Annual AML and Financial Crime Conference—Europe, Workshop A, London, Wednesday, May 31*
- *Mastering the Art of Change: Bolstering Necessary Skills to Introduce and Incorporate Changes into Your Anti-Financial Crime Compliance Program: ACAMS 13th Annual AML and Financial Crime Conference—Europe, WORKSHOP B, London, Wednesday, May 31*
- *CAMS Examination Prep Seminar:* London, Wednesday, May 31, Free to conference attendees
- *ACAMS 13th Annual AML and Financial Crime Conference—Europe, London, June 1-2*

I look forward to seeing you somewhere in Europe in 2017. 🇺🇸

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

SAMANTHA SHEEN, CAMS:

THE CHANGING AML LANDSCAPE IN EUROPE

Samantha Sheen is an anti-financial crime risk professional who joined ACAMS in 2016 as its anti-money laundering (AML) director for Europe. Sheen has worked in both the public and private sectors on a variety of anti-financial crime projects and activities. Sheen's career has afforded her the opportunity to work with global financial institutions and regulators from different jurisdictions. She holds a variety of qualifications including CAMS, a bachelor's degree in public administration and a master's degree in business, specializing in risk management.

Sheen previously worked as the inaugural director of the Financial Crime Division for the Guernsey Financial Services Commission. She joined the Commission in 2010 as its first legal counsel. Prior to joining the Commission, Sheen worked as legal counsel for various financial companies in both Canada and Australia. While in Sydney, Australia, Sheen worked with a large accountancy firm in its compliance advisory team before moving to Guernsey.

Originally from Montreal, Canada, Sheen started her legal career in Toronto in the late 1990s. Sheen's particular area of interest is in relation to the effectiveness of risk management and mitigation measures in influencing changes in staff behavior and culture within financial institutions.

ACAMS Today: What do you look forward to working on as ACAMS' AML director for Europe?

Samantha Sheen: I really look forward to interacting with the many different stakeholders involved in anti-financial crime compliance. Banks, insurance companies, Fintech firms, government regulators and think tanks all have unique and valuable insights

into the challenges posed by financial crime threats and how these threats are addressed.

AT: How has the AML/CTF landscape changed in Europe since you first started working in this industry?

SS: The landscape has changed in a significant way. When I first started, compliance was a subteam of the legal and risk department. Now, each of these areas are specialisms in their own right, but there is always a need to ensure that those areas continue to speak with one another in mitigating financial crime, and not become siloed and work separate from one another.

AT: What challenges are financial crime prevention professionals currently facing in Europe?

SS: Complexity, resourcing and time. The key to being an effective professional in this field is to be not only an adaptability to change, but also changing as a leader. And being receptive to new ways of approaching things, so that performing the role of a compliance professional is achieved by working smarter, and not just harder.

AT: How about globally?

SS: The biggest challenge is the continued disparity between nations in terms of their AML practices. More and more, money laundering takes on a cross-border character, and the ability to identify and prevent this from occurring can be a real challenge when some jurisdictions have different customer due diligence requirements or are limited in their ability to share information due to remaining bank secrecy requirements.



AT: As ACAMS' AML director, what goals do you have for 2017?

SS: My goal for 2017 is to try to reach out to as many compliance professionals as possible about emerging risks and legislative changes, such as the Fourth AML Directive, in a way that helps them to understand those changes (especially here in Europe) and to formulate ideas around how these might affect their existing compliance programs.

AT: What does the future hold for education and training programs for ACAMS members in Europe?

SS: The future is limitless—watch this space!

AT: When you are not working, what do you like to do in your spare time?

SS: Visiting friends and family, taking my two basset hounds for long walks in Greenwich Park and attending the many amazing classical music concerts held by the local university students—and occasionally attending heavy metal concerts. **A**

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

ADVANCED CERTIFICATION GRADUATES

Anguilla

Tessa Oudkerk, CAMS-FCI

Canada

Wing-Chi Leung, CAMS-FCI

Chris Randle, CAMS-FCI

Greece

Joanna Kozłowska, CAMS-FCI

Lebanon

Nadine Abouzeid Harb, CAMS-Audit

United States

Jimmy Brown, CAMS-FCI

Maria Dodson, CAMS-FCI

Katie Foley, CAMS-FCI

Dan H. Jackson, CAMS-Audit

Patrick Kore, CAMS-Audit

Angela Lintag Ihde, CAMS-FCI

Aaron Lloyd, CAMS-FCI

Scot Luther, CAMS-Audit

David E. Martin, CAMS-Audit

John McCormick, CAMS-FCI

Jennifer Morrison, CAMS-Audit

Karen Motley, CAMS-Audit

Jae Park, CAMS-Audit

James Prestopino, CAMS-FCI

Kishani Ratnayake, CAMS-FCI

Christopher Recor, CAMS-Audit

Terri Pelle Sands, CAMS-Audit

Sherri Scott, CAMS-FCI

Sherrie Sessoms, CAMS-FCI

Mary Linda Settle, CAMS-FCI

Celeste Uvanni, CAMS-Audit

R. Joseph Soniat, CAMS-FCI



CAMS GRADUATES: NOVEMBER–JANUARY

Andorra

Sandra Vergens Gonzalez

Antigua and Barbuda

Genel Gould

Aruba

Maureen S. Harms
Marusha Quant

Australia

Joseph Raphael Ancheta
Elena Berkovic
Rogie Ria Bravo
Daniel Calcei
David Coppin
Louise Douglas-Major
Seyed Aminollah Eshghi
Mark Evans
Marc Falkiner
Paul Hurrell
Jia Kuan
Janet McCarthy
Toby Noble
Christopher Schaub
Joshua Smith
Hong Yue

Austria

Tomasz Kurek

Azerbaijan

Kamal Jafarov

Bahamas

Anthinear Braynen
Saran Forbes
Alva Henfield
Tamara Humes-Rolle
Teresa Singleton

Bahrain

Seham Ahmed

Mohammed Aish

Hana Al Murran
Mohamed Alalawi
Mujtaba Alrafei
Ghada Sami Awdi
Khalid Ebrahim Saleh
Sanghamitra Rout

Bangladesh

MD.Alomgir Bashar
Nashid Hassan
Jahidul Islam
Saiful Islam
Tauhidul Islam
Mohammad Wahidul Islam
Mahbub Kader
Kazi Shafiul Azam
M.M. Shaheen

Barbados

Ian C. Clarke
Bernard Thomas

Belgium

Séverine Anciberro
Eda Bulduk Van Kerckhoven
Dmitry Knyazev
Tatiana Kukushkina
Alexandru Pop-Calinescu

Belize

Arlette Arana
George Guerra
Krystal S. Holder

Bermuda

Eve Foster
Andrew Markus
Zakiyah V. Mills
Kondwani Williams

Botswana

Karabo Ndodole
Tshepo Othibetse

Brazil

Leonardo Abate
Neilton Barbosa
Camila Canaverde
Andre M. Dos S. Silvestre
Alexandre P. Gomes Zanetti
Patricia Miguel Gouveia
Gustavo L. Pacifico Peçanha
Priscilla Oliveira Sartori
Lucilene Pires
Vanessa Rafael Vieira
Frederico Wolf

British Virgin Islands

Shanon C. Lawrence
Ajani Skelton
Marsha Vanterpool

Cambodia

Yixuan Li
Hoy Leng Wong

Canada

Marissa Adams
Maleeha Alam
Ali-Jaffer Ansari
Elodie Archambault
Thivagar Arumarajah
Arjankumar Azad
Pawan Bains
Harish Bhonsle
Andre Boutros
Matthew Brikis
Jaqueline Castrillon
Sze Long Daniel Chan
Wa Hin William Chan
Shao Feng (Steven) Chen
Yue Chen
Isabella Cheung
Jessie Cheung
Ken Cheung
Su Jeong Crystal Cho
Marc Cocorocchio
Nadia D'Amario
Saranya Danasekaran
Gregory Draper
David Dunne
Sara Elehky
Abosede Enakimio
Asif Farooqi
Mitchell Finkbeiner
Eric Foote
Marcia Francis
Olivia Fung
Maria Giltsov
Gagandeep Grewal
Michelle Hay
Rita Ho
Patrice Hornstein
Gabor Horvath
Nancy Hurstfield-Meyer
Jeff Jackson
Malik Jaffer
Shahrukh Jafree
Kerizanne Kassarie
Virab Khachatryan
Hee Jin Ko
Wilson Lai
Roberta Lam
Ariane Leduc
Ha Young Amy Lee
Kejun Liu

Anna Maison
Jeffrey Kwan Kit Mak
Ali Malik
Jorge Mencia Urdaneta
Ian Messenger
Bartley Miller
Shivani Misra
Changwe Musonda
Amelia Nandlall
Martin Nigro
Lawrence Oko-Oboh
Alexandra O.-Verlegh
Caroline O'Toole
Jonathan Pang
Diana Pinto
Julie Poirier Longpré
Ada Poon
Karan Popli
Serge Prostran
Krista Randall
Omid Riahiachali
John Ritchie
Kelly Ross
Nichole Salfarlie
Ryan Scavella
Faiza Shaikh
Richard Sharpe
Shahryar Sheikh
Jayong Shin
Steven Sims
Angela Sue-A-Quan
Hsin-Yi Tseng
Debbie Villeneuve
Nils Weidenbruch
Bonnie Kai Yue Yeung
Vanesse Yu

Cayman Islands

Katherine Arch
Kieron Cacho
Sueli Ferreira
Kiara Kerins Shanahan
Kara Owens
Felicia Paddyfoote

Chile

Ricardo Correa
Susana Ester Daure Ortiz

China

Xiao Chang
Yu Chang
Pei Yu Perry Che
Hai Juan Chen
Hang Chen
Hui Chen
Jianbo Chen
Li Chen
Lingyuan Chen
Wei Chen
Xiao Yan Chen
Xiaolong Chen
Yun Ru Tammy Chen
Zui Feng Chen
Libin Cheng
Li-wei Cheng
Deshan Deng
YiHao Deng
Huixu Fan
Xiaoling Fan
Jing Fang
Zijian Fang
Xiaoxiao Fu

Yu Li Gu
Feng Gui Ting
Huayu Guo
Lu Guo
Xiaoxia Guo
Zhilin Guo
Mimi Hao
Bin He
Ling He
Peijian He
Yike He
Jianguo Hu
Tengteng Hu
Wei Hu
Xiao Hu
Jieling Huang
Jing Yi Huang
Na Huang
Pei Qing (Christy) Huang
Xintao Huang
Hongying Huo
Yang Jia
Zhiyi Jie
Chunying Jin
Sihan Jin
Qiong Ju
Wenqi Ke
Sou Fong Leong
Chao Li
Chujun Li
Jia Li
Li Li
Meng Li
Qing Min Li
Shuangfeng Li
Shuting Li
Wan Qi Li
Wenliang Li
Xiaotao Li
Yin Li
Qiu Feng Liang
Xingyu Liang
Yong Jiang Liang
Si Min Lin
Wan Hua Lin
Wanghua Lin
Fengdan Liu
Qiu Fen Liu
Sichen Liu
Xiao Hong Liu
Yuanjia Liu
Xiaoqian Daphne Lu
Haoyuan Luo
Yun Luo
Eric Ma
Jie Ma
Li Lin Mai
Tian Chao Mou
Jian Pan
Yi Wen Pan
Yun Peng
Xue Pu
Haiqiang Qian
Su Qin Qian
Bei Bei Quan
Yamin Rong
Linjing Ruan
Yanying Ruan
Shenyue Rui
Jiejun Shen
Luoxiao Shen
Yuliang Shen
Changlu Shi

Qiong Shi
Yaobin Shu
Lv ShuMei
Dan Song
Haiyang Song
Hongmei Song
Baoyun Sun
Peixiang Sun
Wei Sun
Zhaoguo Sun
Zheyuan Sun
Lichuan Tan
Zhen Kun Tu
Ming Hui Wang
Cong Wang
Dan Wang
Haizhen Wang
Kaihua Wang
Le Jin Wang
Lingyun Wang
Wei Wang
Xiaoli Wang
Xiaoyan Wang
Xin Wang
Xinyun Wang
Xiuping Wang
Xueping Wang
Zhen Wang
Lian Wei
Yusha Wei
Bi Shan Wu
Cui Ying Wu
Heng Wu
Hongyan Wu
Wangyuan Wu
Weiming Wu
Yuanxin Wu
Jingwen Xia
Hui Hui Xiao
Jing Xie
Chunhui Xu
Junwen Xu
Tingting Xu
Bo Yang
Huanhui Yang
Li Lang Yang
Linlin Yang
Ning Yang
Shipeng Yang
Tong Yang
Yang Yang
Yiyang Yang
Zhan Yang
Lei Yao
Qiong Yi
Jinchuan Yin
Hongwei Yu
Xiaofeng Yu
Li Hua Yuan
Chaokai Zhang
Hongxi Zhang
Jian Bin Zhang
Jiang Zhang
Jun Zhang
Lei Zhang
Long Zhang
Peng Zhang
Rui Zhang
Weinan Zhang
Wentao Zhang
Xiaoli Zhang
Zhen Zhen Zhang
Jie Zhao

Nan Zhao
Xue Zhao
Yanlan Zhao
Yuhong Zhao
Zixuan Zhao
Yi Zheng
Zeqian Zheng
Catherine Zhou
Hao Zhou
Heng Zhou
Ting Zhou
Yihui Zhou
Yue Zhou
Lihong Zhu
Lingling Zhu
Yangzi Zhu

Costa Rica

Christopher Morgan Brenes
Jorge A. Rodríguez Calvo
Carlos D. Romero Monge

Croatia

Katarina Pranjić

Curaçao

Jhaheila Granger
Rosa H.-Fernandes Correia

Cyprus

Vasiliki Christodoulou
Marilena Chrysostomou
Thalia Dimitriadou
Maria Hadjivassiliou
Kyriaki Neofytou
Linos Shiakalis
Theodora Theophanous

Czech Republic

Bohustava Mondova

Denmark

Kenneth Carstensen
Tim Nielsen

Egypt

Khaled M. Ali Mohamed
Amr Issa
Hazem Kamel
Tarek Nassar
Michael Raouf Mounir

El Salvador

Henry D. Escamilla Zaladaña
Jose Urrutia
Andres Valiente Thoresen
Ada Raquel Vigil Hernandez

Estonia

Anneli Puusepp

Finland

Jani Samuli
Valtteri Sulonen

France

Irina Baksheva
Anne-Laure Barbosa
James Baxendale
Lucas Boushra
Nathalie de Larminat
Remi Demelle
Anicet Fantar

Henrique Goncalves Alves
Isabelle Grenet
Carole Monnet
Amélie Morin
Romain Nicolas
Baptiste Saint Aubin
Cédrik Schroeder
Thomas Seignovert
Fanny Soysouvanh
Simon Vaughan-Johnson

Germany

Hans-Georg Beyer
Julian Defoe
Desiree Hildmann
Florian Imrics
Bartłomiej Kudlik
Jennifer Petronio
Rebecca Wokittel

Ghana

Enoch Kwesi Amoako
Francis Nyamekye

Greece

Konstantinos Papastergiou
Konstantina Taxaki

Guam

Jessica Atalig
Janice Quichocho

Guyana

Pauline Singh

Haiti

Clarkens Andre

Honduras

Reyna Meza Ruiz

Hong Kong

Thomas Allport
Micheline Archibald
Faith Bhaseen
Francis Brown
Korsan Cevdet
Ching Man Chan
Connie Shuk Ling Chan
Hiu Wai Jennifer Chan
Ho Kwong Chan
Ho Leung Chan
Karen Chan
Man Fai Chan
Marty Chan
Pui Pui Renee Chan
Suk Wah Chan
Sze Nga Chan
Ting Chi Iris Chan
Tung Wah Chan
Wai Kit Chan
Yik Sun Vincent Chan
Yuk Pui Chan
Yu Man Chang
Po Yue Chau
Connie Cheang
Ka Yee Cheng
Man Tak Cheng
Chi Ping Cheung
Ivan King Yan Cheung
Ming Fung Cheung
Sze Mei Cheung

Yuen Shan Cheung
Alvis Chiu
Winnie Chiu
Kai Shing Choi
Lai Sheung Choi
Shun Keung Choi
Suiqun Choi
Wan Zheng Jessica Choi
Mei Po Chong
Suk Fong Linda Chong
Chi Wai Chow
Fung Keung Chow
Pak Ho Chow
Yuk Shun Choy
Chun Chu
Lawson Chu
Po Ying Chu
King Yip Chung
Simon Cook
Paul Critchley
Shangwen Dong
Tsz Mang Fok
Ching Yin Fong
Lee Sze Fung
Shek Fung
Lisa Hansell
David Haynes
Albert Ho
Kin Fan Ho
Lai Kwong Ho
Ming Kit Lily Ho
Siew Chan Ho
Sze Wai Ho
Yui Kuen Ho
Chin Wing Hon
Chit Wai Hu
Sze Ki Hui
Chun Ping Ip
Irene Iu
Xin Jin
Mei Wa Kam
Yuen Kei
Abdul Hameed Khan
Hin Cheung Kung
Siu Kwan Chiu
Chi Hang Kwok
David Kwok
Hoi Lam Kwok
So Yan Kwok
Hon Kit Kwong
Michelle Ming Yan Lai
Pak Hei Lai
Chung Ching Patrick Lam
Kin Leung Lam
Kun Yuen Lam
Pui Sze Lam
Suk Kwan Lam
Tsz Hung Lam
Yee Sheung Isis Lam
Yim Ping Rebecca Lam
Christy Si Lai Lao
Hau Shan Lau
Ho Kan Lau
Kwun Tak Lau
Mei Yi Lau
Ming To Lau
Tsz Kit Felix Lau
Tsz Yeung Ivan Lau
Francois Lauraire
Astor Kit Yee Law
Fook Shan Law
Hoi Ki Law

Ka Po Law
Cheuk Yu Stephen Lee
Hoi Fung Lee
John Lee
Ngok Lung Lee
Yee Sai Lee
Weng Kan Sam Leong
Amen Leung
Eddie King Hung Leung
Hoi Lam Leung
Ka Zin Leung
Kok Chun Leung
Pak Ning Leung
Wilson Leung
Yu Hin Leung
Francis Li
Li Li Li
Shing Him Li
Siu Ho Li
Wing Yan Frenda Li
Chia Hsin Lin
Ka Chun Lin
Yu-Ying Ling
Caster Liu
Tingting Liu
Chi Shun Lo
Ka Chi Lo
Yue Lo
Yui Chuen Lo
Julie Ying Wen Louie
Ho Kit Lui
Janel Jo Yin Lui
Hiu Sum Mak
Wai Kei Gary Man
Colin Ng
Kei Kwong Ng
Oi Yee Ng
Ming Sun Ngai
Alexander Oxford
Yuen Ting Po
Max Rebol
Michael Regan
Pranav Sarkar
Haeyoeun Seo
Sandeep Sharma
Ming Wah Zome Sheung
Tak Pong Shin
Yiu Kuen Shun
Merry Siu
Yan Lun Siu
Suk Han So
Ka Chung Soong
Ka Ki Sun
Steven Tait
Lik Hang Alex Tam
Ming Kai Alan Tam
Yu Fai Tam
Shing Tung Tang
Tat Cheong Tang
Wai Cheung Tang
King Chun To
Radomir Tomovic
Chi Ping Tsang
Samuel Tsang
Wai On Tsang
Margaret Tse
Monida Tse
Kwong Yip Martin Tso
Chun Yuen Tsui
Tracy Hei Yan Tsui
Yam Tsz Kit
Hitesh Vanzara
Linda Hing Fan Wan

Man Kit Wan
Yi Wang
Chung Kwan Wong
Eddy Chi Wai Wong
Ka Lai Wong
Kevin Hiu Sing Wong
Lap Chi Wong
Maggie Wong
Man Shan Shana Wong
Teen Wai Grace Wong
Wai Wong
Yuk Chi Wong
Ka Man Wu
Pui Ling Yan
Shuk Man Yan
Wai Lun Yan
Christina Yeung
Wyatt Yeung
Xiaoqian Yi
Chung Tak Yu
Hiu Mei Yu
Hoi Ting Yu
Joanne Yu
Eddy Yuen
Oi Wah Yuen
Hoi Man Yum
Chi Fung Yung
Chung Man Yung
Qian Zhao

Hungary

Craig Keddie

India

Sneh Deep Agnihotri
Ravi Shankar Aylasomayajula
Vishnu Babu
Gaurav Barad
Neetu Bhatt
Nikhil Bhatt
Swati Budhraj
Sachin Chitrakar
Deepa Chotrani
Nianaaz Darabna
Diya Das Kutty
Taher Dholkawala
Zahir Hirani
Ganesh Iyer
Ajith Jose
Vivek Kapalavai
Parimal Karia
Goldi Kaushik
Sivaguru Krishnamoorthy
Manoj Kumar
Naveen Kumar
Prasoon Kumar
Deepa Lakshmi
Sunil Landge
Sheetal Maliye
Rohit Mehra
Sudheer Menon
Anitha Mukunda
Jagannath Nagarajan
Pramod Nair
Lakshmi P. Panchagnula
Nehal Panchasara
Krishna Parmar
Chandra-Sekhar Patro
Himanshu Pramanick
Byju Puthumana
Vikas Razdan
Poonkoman Rengasamy

Prakash S. Panneerselvam
Sojan Samuel
Ishan Seth
Divij Shah
Pradip Sharma
Shalabh Sharma
Aathi Sivakumar M
Ghanshyam Srivastava
Karri E. Subrahmanyamu
Rengaraj Suresh
Sabina Syed
Ameeta Dev Tandon
Vijayaganesh T. Vijayaraghavan
Vijaya Udayasankar
Venugopal Vempati
Sathya N. Venugopal
Tushar Verma
Ankit Vora

Indonesia

Jessica Siau
Aditya Putra Utama
Edwin Widjaja

Iraq

Tameem Kareem Hayyaw

Ireland

Mark Bonham
David Collins
Patrick Coyne
Katarina Milakovic
Dermot O'Reilly
Malavika Sivasankaran

Israel

Uri Tolkowsky

Italy

Sergio Luciani
Maria Silvia Pau
Giuseppe Sollazzo
Tao Yang

Jamaica

Maxlyn Noble

Japan

Yasushi Aoki
Yuya Aoki
Hiroshi Araki
Yusuke Araki
Shigeru Hashimoto
Masanobu Honda
Kozue Kato
Sunao Katou
Kazuhiko Katsube
Naomi Kodama
Masami Koike
Takanobu Komori
Emi Matsuoka
Satoshi Midorikawa
Shinsuke Mitsui
Yasushi Miyano
Takayuki Mochizuki
Yoshitaka Mori
Satoko Nakamura
Soushi Nakao
Akiko Noguchi
Aoi O'Brien
Keiko Ogawa
Keiko Ono

Yurika Ono
Kyo Onodera
Shinji Osumi
Momoko Sako
Yoshio Sasahira
Takashi Sasaki
Taso Tadatoshi
Makoto Tagaya
Kazue Tanaka
Koshi Tanaka
Emi Uchizumi
Keishi Urakami
Kei Watanabe
Yoshiaki Yamamoto

Jordan

Mohsin Ali Abbas Alzuabidi
Nader Abu Mayyaleh
Issam Ahmed Ali
Nizar Al-Asal
Sewar Al-Dababneh
Riyad S. Ibrahim Alsalwalmeh
Mohammad Alaffi
Ismail Al-Hourani
Farah Issam Salih Aljanabi
Ali Al-Msarwhe
Tamara Alnsour
Ali Abdulkareem Aloufi
Yousef Aqel
Sami Abdullah Ashour
Husam Assaf
Hayder Hassan Hayder
Neven M. Ibrahim Azmi
Amal Jaber
Sara Khair
Raad Makableh
Rudina Malkawi
Mohammed K. Mohammed
Ali Mohammed Atta
Awais Mustafa Yousef Muti
Jamal Obeidat
Waheed Qar'a
Yasir Muwafaq Sami Al-Najm
Fayez Shraim
Rula Zakaria

Kazakhstan

Baglanuly Aidar
Yerkebulan Ashirov
Baidybekov D. Malikovich
Azamatova K. Kairatkyzy
Kanysh O. Kuanbayev
Timur Mussin
B. S. Omarkhanovich

Kenya

David Githecha
Jonah Kangogo
Argwings Koyoson
Andrew Karanja Kung'u
Agnes Magero
Pascal Manthi
Anne Matu
Grace Mburu
Victor Musyoka
Leonard Mwangi

Kuwait

Mudawi Al-Othman
Raymond Joseph
John Simon
Peter Tawfeek

Mithun Thalakkal

Laos

Hongtao Mao
Somvone Siaphay

Latvia

Vija Arsenjeva
Janis Brazovskis
Vjaceslavs Budjakovs
Daina Busmane
Kaspars Dreimanis
Jevgenijs Fisenko
Ruslans Gorodovs
Ilja Gutkins
Diana Jeremejeva
Ksenija Kercgure
Jelena Kibale
Julija Lazarcuka
Aira Magone
Aleksandrs Paze
Ilze Petersons
Marina Pikina
Konstantins Skorohodovs
Vladens Topcijans
Olga Volkova

Lebanon

Grace Bdaywi
Ali Beydoun
Khaled Chahine
Dima Fakhoury
Bahaa Hamwi
Elias Hanna
Tony Janho
Amal Kayss Chaaban
Randa Manih Ramadan
Sylvain Massaad
Rafi Mawla
Sarkis Mazraani
Saria M. Kheir Traboulsi

Lithuania

Ruta Andrijaityte
Konstantinos Angelou
Gintaras Butenas
Egle Palecke
Agniete Serelyte
Brigita Vaitiekune

Luxembourg

Eduard Amroyan
Rui Gaspar
Qian Li
Philippe Muller
Jonathan Seitz
Barnaby Taylor

Macau

Chan Hoi Chan
Chi Wa Chan
Choi San Chan
Fai Hou Chan
Ka Chon Chan
Lai Ha Chan
Lai Man Chan
Nga In Chan
Pek Kuan Chan
Pou Ian Chan
Pui Lan Chan
Sio In Chan
Sio Wai Chan

Soo Chung Chan
Sut Lin Chan
Wai Pan Chan
Ka Chon Cheang
Wai Chan Cheng
Kam Sio Cheok
Meng Po Cheong
San San Cheong
Wai Mei Cheong
Pui Wan Chio
Sin Keong Chio
Chan Wa Choi
Ieng Chi Choi
Joey Chi Kit Chong
Weng Fat Chou
Sou Fai Wong
Chin Hin Fok
Lai Fong Fong
Sio In Fong
Ka Chong Ha
Lai Tong Ho
Ka Wai Hoi
Ka Weng Hoi
Kong Hong Hoi
Man Chon Hoi
Oi Ping Hung
Lai Ieng Iao
Ku Iao Mei
Leng Chan Ieong
San Weng Ieong
Leong Im Wa
Jiayi Jiang
Weng Si Kam
Wong Kam Chao
Ho Kam Peng
I Man Kong
Wai Hong Kong
Mei Kei Kou
Hang I Ku
Lo Kan Ku
Sin Ieng Ku
Kim Pan Kuan
Sok Mui Kuan
Man Wa Kuok
Hio In Lai
Ho Ho Lai
Fong Hou Lam
Lai Man Lam
Chio I Lao
Hoi Ian Lao
Chi Iat Lei
Chi Lon Lei
Hou Io Lei
Man Sin Lei
Mei Fong Lei
On Teng Lei
Chin Fai Leong
Heong Tong Leong
I Lam Leong
Ivo Leong
Meng Kuan Leong
Jiali Li
Jiaying Li
Lu Liu
Yan Liu
Ka Lei Lo
Chuhong Lu
Jinyang Luo
Chon Chi Ma
Tan Leng Ma
I I Ng
I Ian Ng
Kam Hin Ng

Seng Ut Ng
Wai Man Ng
Iek Hang Ngan
Yukichi Ogata
Ricky Weng Kun Pao
Jie Ren
Heng On Sam
Hou Fai Sam
Oi Ian Seng
Chang Shu
Chong Lei Si
Hoi Ian Si
U Sam Sio
Cheok Heing Siu Lei
Ha Chao Sou
Hao Leng Sou
Kun Su
Chong Fai Tai
Io Chou Tai
Minzhi Tan
Fong Koi Tong
Ka Fai Tou
Chan Leong U
Ka Ian Cecilia Vong
Chang Hsiang Wang
Jue Wang
Li Wang
Kio Fong Wat
Leong Weng Nga
Cheng Hou Wong
Chi Iong Wong
Fong Wong
Ieok In Wong
In Meng Wong
Ka Hou Wong
Pui San Wong
Sio Ian Wong
Sun Lap Wong
Un Fai Wong
Wai Heng Wong
Yuehui Xu
Cuiying Ye
Cheng Yu
Jing Zhang
Peiling Zhang
Xiao Min Zheng
Junyuan Zhu
Xinwei Zhu

Malaysia

Magdalena Brzuszkiewicz
Kwai Fun Chia
Puteri F. D. Mustapha Rounal
Rohini Sivarajah
Sivakami Sundararajan

Mexico

Aquiles Carrillo Flores
Maicon Luis De Castro
Gerardo Espinoza Arias
Eleazar Gaona Figueroa
Priscilla Manzo Santa Cruz
Marina G. Martinez Jimenez
Mireya Valverde Okon

Moldova

Stela Recean

Namibia

Siyabonga Madonsela
Alfred van Rooi

Nepal

Rajesh Bastola
Vishal Rauniyar

Netherlands

Evelyn Bell
Clyde Korsten
Zuzanna Marczak
Sarina Molenkamp
Wytse Schukken
Seema Shahi
Maureen Wernet

New Zealand

Jianping Cai
Judith Caskey
Roger Clarke
Lena da Fonseca
Su Jin Zhong Lau
Michelle Moore
Dennis Parsons
Petrus Visser

Nigeria

Oluwaseun Agbato
Olajide Akinlonu
Olanike Alao
Ugochukwu Okeke
Adesina Titilope Motunrayo

Oman

Saikumar Sukumaran

Pakistan

Zartash Sultan

Panama

Raltom Villar
Vielka Villarreal Villagra

Paraguay

Gustavo Garcia

Peru

Diana Arreluce Garrido

Philippines

Genevieve T. G. Alcancia
Heinz Ryan Espinosa
Leah Hernandez
Kathryn Ramos
Jose Luis Syquia

Poland

Malgorzata Bieszke
Sergiusz Byczkowski
Melissa Carneiro Kobus
Monika Ergun
Jan Schwartz
Xiaohui Wang

Portugal

Paula Borges

Puerto Rico

Melissa De La Torre Vasquez
Luana Santos Burgos

Qatar

Ezzalden Abu-Sitta
Javed Akhtar
Wei Gao

Minglei Sun
Guangxin Wang
Shaune Williamson

Saint Kitts and Nevis

Steve Farier

Saint Vincent and the Grenadines

Isaac Solomon
Grenville T. Williams

Samoa

Siavata Nofoaiga

Saudi Arabia

Latefah Abdulrag Al Khlaf
Abdullah Bin Khamees

Singapore

Kamilah N. B. Abdul Ghafar
Sindhujia Arumugam
Shiv Shankar Barasia
Dirk Carstens
Kai Wai Chan
Yu-Ping Chen
Yuping Chen
Hui Lee Rachel Cheng
Tan Cheng Wah Bobby
Man Yee Cheung
Ting Fung Cheung
Wei Qiang Choo
Tzu Chou
Kenny Chow
Cheng Shen Eugene Chua
Sharad Cyriac
Ahmed Drissi
Johnson Ebenezer
Yew Heng Raymond Han
Alistair Hawes
Darren Lungqing Darren Ho
Ellen Chen Huey Ho
Wei Yee Hoi
Melissa Huang
Alvin Yu Cheng Hui
Feng Jia Kiew
Annabell Koh
Siew Tin Joey Koh
Xin Yun Koh
Jun Hao Joshua Kong
Lai Mei Ku
Ee Fung Alicia Lau
Andrew Leow
Pei Ling Lim
Pei Shan Lim
Scott Loh
Abhishek Loha
Keith Loo
Kella Murthy
Wei Cheng Danny Neo
Pey Wen Ng
Shauna Tze-Yin Ng
Wei Khim Ng
Siew Hian Summer Ngoh
Sui San Oei
Yi Lin Ong
Ujjal Pakrasi
Rui Pan
Tan Hui Ping
RenWei Poh
Prabhat Ranjan
Pei Chen Saw

Smita Sequeira
Sunil Sharma
Kechang She
M. Shunmugasundaram
Jacqueline Sng
Kshatriya Mohan Srinivas
Nithyanandha Subramanya
Mohammed M. S. A. Wahab
Angela Wan Yin Tan
Honey Tan
Siew Gan Tan
Burzeen Tengra
Bryan Wei Jian Teo
Janet Pei Ling Teo
Roy Teoh
Kairong Toh
Jonathan Wee
Jayson Hoe Meng Wong
Kim Har Wong
Lynette Wong
Wei Ching Wong
Shi Hui Woon
Lok Yu Wu
Tingxuan Kenneth Xiao
Weichao Xu
Hui Yan
Eugene Yap
Hazel Yeo
Kai Wen Yeo
Zhenrong Richard Yeong
Yixiang Yow
Qiao Yun Lim
Qi Zhang
Owyang Zhiyan
Yufan Zhuo

South Africa

Warren Baas
Keith Botha
Ming Cheng
Annalisa Contrafatto
Yuliya Doroshenko
Graciela Gonzalez Brigas
Jaco Herselman
Jurie Aubrey Kok
Zuren Liao
Colin Maluleke
Kriya Mohan
Divinia Naidu
Robert Nel
Kamini Reddy
Quinton Stone
Werner Venter

South Korea

Yun Hee Cho
Suk Joon Ko
Young-Ho Nam
Eun Ok Noh
Jean Park
Soyoon Yoon

Spain

Antonio S. Manzhirova

Sri Lanka

Irantha Abeyratne
Sachini Mahaulpatha
Sasika Morawaka
Kariyawasam Nimanthi
Helamba A. D. P. Perera
Dhanushka S. Weerasinghe

Sweden

Anna Bülou
Anna Wingårdh

Switzerland

Tatiana Belyaevskaya
Julia Brand
Gabriel Brunner
Elina Comment
Olivia Iwicki
Roxana Savulescu
Angelica Sola
Natalia Stolyga

Taiwan

Chia-Wen Chen
Chih Peng Chen
Kuan-Rong Chen
Kuo-Chih Chen
Kuo-Hsien Chien
Chang Yun Chu
Chiu Yen Chu
Fang-Yi Chu
Chuan-Yuan Chuang
Chun Te Ho
Leon Ho
Hsueh-Ni Hsieh
Benjamin S.-Hsiang Huang
Elly Yai Huang
Yu-Ting Huang
Wanlin Kuo
Yi Ju Kuo
Yung Cheng Kuo
Rico Ming Kit Kwong
Angel Mi Lee
Chen Ni Lin
Hui Jen Claire Lin
Wen-Yu Lin
Hsiu-Chuan Liu
Chang-Heng (Clement) Lu
Wei-Ping Lu
Shiao Ching Peng
Yu Ti Peng
Li-Chen Tai
Wen Tien
Ai Ling Tsai
Chao-Ping Wu
Dickson Yang
Ming Tsung Yang

Tanzania

Elias Mushi

Thailand

Saovaporn Sattabusya
Naphat Triphan

Trinidad and Tobago

Ahamad A Z Hosein
Simone Bayley
Yejiide Che-Quile Liverpool
Marika Manswell
Reema Ramnanan
Maureen Scott

Turkey

Bahtigul Akin

Turks and Caicos Islands

Rebecca Gibson
Melissa Prosper
Tamiko Smith

United Arab Emirates

Salwat Ahmad
Ranya Ahmed
Sherin Ahmed
Tanbir Ahmed
Abdulaziz Al-Hashmi
Hamda Alsarkal
Rona Alteza
Imtiaz Ahmad Ansari
Archana Banger
Roy Daccache
Eric Dagenais
Pinaki Datta
Sindhu Devi Villa
Zouhair El Moutaraji
Wael El-Nagar
Michel Farah
Janice Fernandes
Kazi Hossain
Hina Imran
Narayan Iyer
Syed Ali Jafri
Prashanth Janarthanan
Jikesh Jayan
Vibhu Joshi
Muhammad Rizwan Khan
Aysha Khurram
Xiangjun Kong
Reema Kunhimangalam
Mirza Lisica
Hasnain Mehboob Damani
Fahmeeda Aftab Merchant
Ali Akber Yasukai Khan Mirza
Archana Mohan
Raza Oshim
Veera V. U. Pamidimukala
Saad Qureshi
Narendran Ramachandran
Syed M. Hussain Rizvi
N. Jayanth Sarathi
Anil Sethi
Athar Ali Shaikh
Shaloo Sharma
Abdul K. Sheik Dawood
Meena Shivnani
Arunabh Kumar Singh
Mehmet Yuksel

United Kingdom

Ahmed Abdullah
Lloyd Agbandje
Alvaro Aguilar Camacho
David Barnes
Paulette Basse
Richard Brough
Claire Burrells
Jasraj Cheema
Wing Yin Chong
Malgorzata Cieslinska
Paul Craigie
Stephen Cummins
Mireya De Jesus Mirelles
Harry Evans
Suresh Fernando
Helena Fortes
Annegret Funke
Katherine Gormley
Xianjun Gu
Ize Idemudia
Andrew Jackson
Saanya Jain
Mondiui Jaiyesimi
Christopher John Johnson
Mohamad Kabbani
Mohamed Amine Kabous
Jeremy Kanarek
Laura King
Rachel King
Kiran Kohli
Stephanie Letessier
Nicholas Li
Alison Mackey
George Maddock
James Maddock
Soumia Majumdar-Dey
Rachel Marsh
Michael McInnes
Mba Nmaju
Daniel O'Sullivan
Christel Pan Yan
Taminder Pattar
Hannah Pitchford
Tessa Potter
Syama Prakash
Stephen Purdie
Alshafia Rahman
Stanley-Paul Ransford
Jean Sebastien Rayo
Conrad Rhodes
Thomas Rixson
Ben Robbins
Janine Ross
Ravinder Saini
Thomas Shipley
Karolina Struminikovski
Bablu Subhan
Asim Sultan
Olivier Tchoumi
Bruno Viana Gomes
Xiaoqing Wang
Gulli Zaripova
Halyna Zenhel

United States

Ahmed Abdulai
Bridget Abraham
Ibelise Acosta
Elizabeth Acosta Aceves
Evan Addison
Stanley Addo
Ruth Adell
Vera Adelschina
Zebiba Adem
Ashley Adler
Rosalina Aggrey
Astor Agosto
Rony Aguirre
Abhishek Aiyangar
Kehinde Ajetunmobi
Shafinaz Alam
Helen Catherine Alber
Madeleine Allen
Laura Almeda
Gustavo A. A. Rodriguez
Amy Alva
Adrian Alvaranga
Jo-Anne Alvarez
Brett Ambrose
Kyle Anderson
Tracy Angulo
Morgan Appezzato
Emily Aquino
Sirarpi Armani-Musaian
Anne-Marie Asare
Ohimai Asein

Phylicia Augustin
Anshu Aujla
Suzanne Auriemmo
Shawna Avey
Nandhini Babu Ayyalu
Keith Babiasz
Amy Baker
Daniel Balsamo
Cory Barghini
Daniel Barlow
Caitlin Barnett
Julie Barns
Jayeeta Basu
Brett Bauer
Bruce Baughman
Kathleen Beck
Jody Beddingfield
Sonja Benner
Kate Bentley
Elisabete Berninon
Marc Bertucci
Aditi Bidaye
Timothy Biddle
Troy Birdyshaw
Elizabeth Birtodaso
Michael Bizanos
Jennifer Bleick
Anna Blenkle-Skomial
Emma Blocker
Jeremy Bloxson
Michelee Bochniarz
Jillian Bolduc
Anderson Bostic
Steven Botinas
Steven Botto
John Boudreau
Sean Bowden
Youlia Bowerman
Jacquelyn Bowman
Tricia Bowring
Antonio Brasse
Margaret Braun
Matthew Brennan
Rochelle Brenner
Dwane Brewster
Tyronne Briscoe
Robert Brodell
Jennifer Broesder
Melissa Brommer
Amy Brown
Ashley Brown
Frank Brown
Heather Brown
Matthew Brown
Rick Brown
Susan Brown
Michael Buholtz
Maud Bui
Carleen Bully-Roche
Christopher Burdick
Parkins Burger
Joseph Burke
Cyndi Burns
Sean Burrows
Jeremy Burton
Sinead Bush
Timothy Callahan
Nancy Camacho
Anthony Canovali
William Cardinale
Sheree R. Dawn Carmichael
Carol Carroll
Francis Cassidy

Erwin Castaneda
Tracy Castle
Pauline Castro
Jules Catral
Joshua Cefkin
Robert Cerviello
Yue Chai
Anna Chandler
Kimberly Chapman
Omar-John Chavez
Jessica Chen
Qiuyue Chen
Natasha Chesness
Prashant Chhipa
Jessica Chiu
Yuliya Chizhov
Wai Shan Chu
Chi Chung
Stewart Cincotta
Nicholas Cipriani
Suzanne Clarke
Valerie Cleveland
Robert Cloud
Tucker Cluett
Sutheeda Cohn
Cynthia Coleman
James Collins
Lisa Connell
Matthew Conrad
Ma. J. Nicole Corrales
Melissa Cortes
Timothy Courtney
Nick Cox
Sophie Coy
Thomas Criscuolo
Patrick Cronin
Natalie Cross
Magdalena Cupo
Daniel Curley
Amanda Curtis
Blake Daubenmire
John Dauser
Courtney Davis
Marcos De Frias
Martijn de Graaf
Nicholas De Silvio
Lyle Deepe
Pamela Dees
Benjamin Defibaugh
Dusty Degreenia
Stephen Delaney
Jacquelyn Delcamp
Hilary DeLorenzo
Justin Demko
Alexander Deniston
Emily Dent
Brently DePriest
Michelle Derham
Susan Deskin
Thomas Dessalet
Suzanne Desveaux
Toby Deyle
Varinder Dhaliwal
John Dickenson
Erika Digeronimo
Tiffany Dindial Khan
Shiqi Ding
Katherine Dodson
Tanner Dorman
Gichard Dormevil
Karl Dorsey
James Duffy
Saurabh Duggal

Ashley Dugger
Luciana Echarren
Daniel Edmonds
Ian Edwards
Thadeous Edwards
Karie Eichenberger
Avraham Elewitz
Ann-Marie Erwin
Carina Espinoza
Scott Estes
Claire Etter
Flora Ezeanaka
Erin Fahey
Aaron Farias
Robert Farquhar
John Fauteux
Brian Fee
Jennifer Fernandez
William Ferrand
Erin Ferris
Lindsay Fletcher
Priscilla Flowers
Darrell Floyd
Abraham Fu
Dariela Fuentes Luna
Adam Furman
Geoffrey Gabriel
Maryann Gallagher
Joel Robert Garcia
Juan Garcia
Anthony Garrett
Adrienne Gaud
Lusana Gee
Brian Gentile
Alexandra Gervase
Jared Getchonis
Michael Gil
Steve Gilbert
Maggie Gill
Sonia Gill
Alfa Giron
Jenna Girouard
Jerry Glasscock
Daniel Glenn
Mary Goff
Paige Goldberg
Juan Pablo Gomez
Israel Gonzalez
Barbara Gottschalk
Jonathan Gouvion
Amanda Graham
Joseph Graham
Damon Gray
Ron Green
Katarzyna Greszka
Georgianna Grey
Emily Griffin
Suren Grigoryan
Benjamin I Grother
Emily Grupp
Eduardo Guardado
Nicole Guess
Brad Gullett
Upul Gunasekera
Aruna Guneratne
Gaurav Gupta
Hyunjeong Gwon
Hayal Habtegiorgis
Jason Halverson
Kevin Hannah
Claire Hanselmann
Amanda Hansen
Ryan Hansol

James Hartnett
Ericka Hashi
Rabia Hassan
Douglas Hattaway
Zana Haxha Begolli
Maolin He
William Tyler Hebenstreit
Paivi Heikkinen-Shah
Kyle Heitman
Timothy Herlihy
David Hernandez
Douglas Hernandez
Jo Ann Hernandez
Josh Herrera
David Hess
Charlie Hettler
Wendy L. Hetzel
Jamie Hidalgo
Dawn Higley
Takesha Hill
Brenda Hinton-Miller
Denise Hoffman-Martinez
Kyle Hoidal
Jason Hollingsworth
Sarah Hollis
Latonya Hollis-Eimerman
Kenneth Holt
Doron Holzer
Madhuri H. H. Ramachandra
Erika Hough
Lisa Hower
Terri Hoyt
Zhiyu Huang
Elijah Ige
Olga Iovcheva
Linda Irerua
Oliver Jahn
Varun Jain
William Jannace
Anter Jatta
Joshua Jedwab
Deirdre Jennings
Barbara Jette
Tianli (Kelley) Jiang
Andrea Johnson
Brett Johnson
Megan Johnson
Tina Johnson
Cassandra Jones
Marsha Jones
Abhijeet Joshi
Ashley S. Kahl
John Kaminsky
Caitlin Kane
Jared Kary
Joseph Keary
Niall Keeley
Nina Kelleher
Sarah Kernagis
Hasmik Keshishyan
Shams Noor Khandkar
Nora Khath
Seeta Khemraj
John Kim
Judith Kim
Se Hwa Kim
David Kimball
David Kincade
Douglas King
Dwayne King
Lindsey King
Scott King
Kelly Kirchner

Matthew Klimek
Brooke Kluepfel
Kompheak Koeut
Aleksandr Koltsov
Anthony Kooistra
Carolyn Koonts
Steve M. Koziol
Briana Kresic
Brittany Krug
Ashish Kumar
Justin Kurian
Elizabeth Kwok
Tammy Lam
Adriana Lamar Pruit
Danny Lane
Nathaniel Lange
Bernabe Laudin
Cuong Le
Michael Lebedovych
Richard Lebel
Ivy Lee
Jane Lee
Christopher Lee-Chue
David Leung
Samson Leung
Sheri Levine-Shea
Jonathan Yao-Rong Li
Mengshi Li
Francisco J. Liang
Barth Lilly
Charles Lin
Frank Lin
James Lindquist
Michael Linsalata
Jawan Little
Aaron Littleton
Alexander Litvinov
Kevin Liu
Pi Kai Liu
Qi Liu
Allan Llarena
Nialanda Lloyd
Jesus Loaiza
Lucas Lockhart
Hayley Logan
Chasity Long
Timothy Lopas
Adriana Lopez
Matias Lopez
Wilson Lopez
Francisco Lorca Susino
Michael Loughnane
Juan Lozada-Leoni
Ryan Lubbers
Grant Lucas
Omar Lucero
David Lugiai
Sheilla Luma
Brandis Lyn
William MacMillan
Kristin Madden
Nicole Maggio
Sola Majolagbe
Moses Makaiwi IV
Indra Mallcott
Jennifer Malone
Maureen Mangilit
Bridget Maresca
Paul Marszalek
Jerry Martin
Joseph Martin
Miguel Martinez
Robert Martinez

Benson Mathew
Cameron Matthews
Megan Matvichuk
Robert Mauro
Allison Maykuth
Mary McAnally
LaShonda McCoy
James Mcdaniel
Ryan McGrath
Ryan McInerny
Tiffany McKinnely
Kimberly McMurdo
Cameron McMurtrey
Carole McNaught
Bryan McNees
Alap Mehta
Thomas Mele
Ryan Menke
Caitlin Mercier
Wladimir Meskelis
Alicia Messick
Gillian Meyer
Javier Meza
William Micho
Robert Michta
Philip Mijares
Elijah Millar
Steve Miller
Marcie Minernd
Sharon Mint
Arden Mitchell
Hasan Mithiborwala
Abdur Mohammed
Christina M. Gad-Ibrahim
Grissel Molina
David Monaco
Andrew Monterrosa
Mary Montgomery
Ashleigh Mooij
Joseph Moore
Alexander More
Kandye Morgan
Sam Moses
Vera Motta
Frashiah Muiruri
Marisa Muller
Christopher Mullins
Bukanya Paul Muwonge
Agnieszka Mycka-Nunez
Michael Myllek
Zulqar Nain
Alan Nakamura
Ruby Nava
Michael Navarrete
Biswajit Nayak
Katherine Nazareth
Daniel Neal
Sharlene Negron
Jody Nesbitt
Aiyana Newman
Flora Ng
Iman Ng
Thomas Ng
Tien Nguyen
Shellie Nimrodi
Terra Noble
Jose Nolasco
Durrell Norman
Michiko Nozawa-Joffe
Evelyn Nunez-Ochoa
Michele Nye
Abdirahman Obsie
Louise O'Connell

Luise Odenheimer
Stephanie Oliver
Edwin Oloo
Lauren O'Loughlin
Brian O'Malley
Jesus Ornelas
Tracey O'Sullivan
Victor Owuor
Mavis Owusu
Namrata Packirisamy
Lisa Pandolfo
Gigliola Pantelidis
Frank Paparelli
Michelle Parham
Kimberly Park
David Parker
Cameron Parrish
Neil Parrott
Robert Pascoli
Michael Pastran Montoya
Devvrat Patel
Neel Patel
Dominique Patrick
Christopher Patzelt-Russo
Bart Pawlowski
Michael Pease
Mark Peckham
David Pedraza
James Pegues
Ricardo Penaranda
Katlynn Pentecoste
Martin Pereyra
Fabian Perez
Niki Perkins
Paul Petrashko
Alexander Petrone
Nicole Pfeil
Caitlin Piasecki
Marianne Pickel
Gloria Pilarte
Kimberly Pino
Luke Poeschl
Lauren Porretta
Angela Powell
Sagun Prabhu Moye
David Prisaznuk
Michael Purvis
Deleana Quan
Thomas Quint
Robert Quito
Megan Racine
Seetharaman Raghuraman
Roderick Ragland
Sneha Raman
Mariel Ramirez
Nickolas Ramsay
Vincenzo Ranauto
J.P. Rankin
Joseph Ransom
Marc Rapuano
Martin Reap
Paige Redd
Angel Reed
Justin Reeder
Marilyn Remedios
Art Reyes
Hector Reyes
Michael Reynolds
Timothy Richardson
Patrick Richers
Manuel Rincon Suarez
Sabrina Rios

Carlos Rivera
Keisha Rivers
Chrishani Rodrigo
Maximiliano Rodrigues
Cristina Rodriguez
Jose Rodriguez
Terryann Rodriguez
Elizabeth Rodriguez Colón
William Rogan
Alice Rojas
Fabiola Rojas
Jorge Rojas
Matthew Rooney
Gabriela Rosas
Matt Rosen
Taylor Rowe
Kirk Rueckmann
Shawn Rullie
Briana Russell
Cindy Rutenbur
Terry Saiter
Tamsir Samb
Ronald Sampson
Victor Samuel
Fausto Sanchez
Deric Sandel
Bryan Sanford
Michael Santiago
Leticia Santos
Samridhi (Sam) Sarin
Gautam Sarkar
Veronica Sarrabayrouse
Norman Sawyer
Kathy Schiller
Kimberly Schipf
Zachary Schneider
Bret Schofield
Trisha Schreier
Jerallynn Schultz
Harley Schultz
Scott Schwartz
Jeremy Seal
Clarice See
Letty Segura
Richard Serrano
Steve Severin
Yelena Shapiro
Akshata Sharma
April Shenk
Jennifer Shimer
Michael Shockey
Rita Shoemaker
David Short
Alexis Shupak
Amy Simmons
Danielle Simon
Jonathan Simon
Peter Singer
Chandra Singh
Rosalayn Singh
Vishalvikrant Singh
Lesia Skarlot
Nicole Sliger
Christine Smitanich
Monique Smith
Rabonne Smith
Stacey Sobbe
Alicia Sorensen
Carlos Sosa
Matthew Sousa
Halima Sow
Nicole Sparago
Osment Spencer

Aaron Spivey
Matthew D. Stalla
Alexis Stanley
Alina Stanley
Levi Stanley
Emily Stevenson
Max Strang
Yokota Strong
Caitlin Stumpf
Romika Subba
Elena Sulimenko
Karin Sullivan
Stephen Sullivan
Jihyung Sur
Noah Swad
Cheria Swan
Cathy Swindell-Smith
Penny Swindle
Ann Sylvester
Anna Tachkova
Nithin Reddy Tadisina
Christopher Talbot
Ashon Taylor
Marshelle Taylor
Zanella Taylor
Jessica Teller
Nathalie Ten Oever
Thomas Tepley
Brian Terranova
Gagik Ter-Sargsyan
Kami Teters
Denise Thomas
James Thomas
Kristen Thomas Biesiadecki
Carena Thompson
Daniel Thompson
Janice Thompson
John Thompson
Nicole Thornburg
Xueqin Tian
Ryan Tite
Richard To
Marian Todd
Marc Toomey
Gregory Topp
Richard Torres
Amy Tostrup
Frederic Toussaint
Christian Javier Townsend
Eduard Trenary
Michelle Triggiani
Frank Tumminia
Kamila Tyburska
Sheree Ulmer
Chinwe Uzoh-Onuorah
David Vail
Rochelle M Valdez
Paz Valencia
Olena Valko
Bradley Vamos
Claudia Vargas
Juan Vargas
Alexis Vasquez
Brandi Ver Ploegh
Gabriela Vera
Hazel Vergaralope
Oksana Verma
Stephanie Villanueva
Tram Vo
Norman Von Seggern
Andrew Walek
Sam Wandolowski

Jenny Ward
Gary Watson
Juma Waugh
Lacey Weimhold
Jonathan Weinberg
Larry Welch
Anna Wheland
Lisa Wichman
LaNeicha Wiggins-Trent
Ellen Willard
Alison Williams
Kim Williams
Michelle Williams
Michael Willis
Brandon Wilson
Daniel Wilson
John Wilson
James Withrow
Matthew Witt
James Woodford
Dean Woodson
Olivia Wozniak
Kimberlee Wright
Chelsea Wu
Guangning Xu
Thomas Yan
Chin Chun Yang
David Yates
John Yates
Ngai Shing Yau
Sam Yong
David Yoo
Cheng Yu
Hansen (Fanfei) Yu
Jason Yu
Dsu-Wei Yuen
Lena Yutsis
Anisuz Zaman
Monica Zapadinsky
Matthew Zavodnik
Dan Zhang
Eunice Zhao
Huasong Zhou
Charles Zidek
Riccardo Zuppelli
Andrew Zyvoloski

Uruguay

Valentina Larrobla
Adriana Perera Kurucz

Vietnam

Ye Lin Li
Hoa Thi Ngoc Tran
Trang Tran Thi Huyen

Zambia

Namasiku Mukaya

Zimbabwe

Precious Chigonga
Poncio Chikati
Wonder Kapofu
Jeffrey Mugwagwa
Colin Mutambira
Fidelis Taziwa

YOUR AD HERE

Don't miss your opportunity
to reach a readership of over
40,000 AML professionals

TO ADVERTISE HERE CONTACT:

ANDREA WINTER

1.786.871.3030

AWINTER@ACAMS.ORG

Mark
Your
Calendars!



Find your next job opportunity!

ACAMS Virtual Career Fair An Online Event

Tuesday, April 18, 2017
12:00 p.m. to 3:00 p.m. EDT

Compliance careers are hotter than ever and employers are seeking top talent. Register now for the ACAMS Virtual Career Fair to network with representatives from top financial institutions.

This recruiting event is free and easy to join!

How it works:

- Choose which employers to interact with and then engage in a direct chat with a recruiter at those organizations.
- Following your chat interview, you'll be able to return to the Event Lobby and chat with other participating companies!

Register today at: <http://careers.acams.org>