

ANNUAL CONFERENCE EDITION

ACAMSTODAY

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

How risky is your risk assessment?

26

A deep dive into country risk assessment

36

SEPTEMBER-
NOVEMBER 2013
VOL. 12 NO. 4

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

www.ACAMS.org

www.ACAMSToday.org

PATRIOT OFFICER®

#1 BSA/AML/OFAC/FACTA/UGEA/SOX/EARA/AIBE/ANTI-FRAUD

Endorsed By The Largest Bankers Associations and Has Passed Examinations

“THOUSANDS OF TIMES”

Financial
Intelligence
Center



Compliance
Network
UCEN.net



Wyoming Bankers Association



GlobalVision Systems, Inc.

9401 Oakdale Avenue, Chatsworth, CA 91311

Phone: (818) 998-7851 Website: www.gv-systems.com

Endorsed by the American Bankers Association through its subsidiary, the Corporation for American Banking

ACAMS 12th Annual

AML & Financial Crime CONFERENCE

SEPTEMBER 23–25, 2013

Can't leave the office? Attend the conference virtually



Comprehensive Training

- Watch live streaming of keynote addresses, plenary sessions and seminars
- Submit questions to the live presenters through your computer
- Gain unlimited access to on-demand recordings of conference sessions after the event

Professional Development

- Receive a certificate of participation and 16 CAMS credits

Interactive Networking

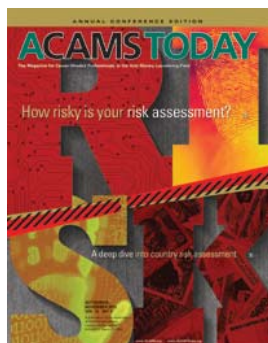
- Share your compliance challenges while chatting with fellow online participants
- Stay updated and connect with your peers via social media platforms

Maximize ROI

- Benefit from top-quality training with zero travel time and minimal expense
- Save on attendance with substantial discounts available for teams

For details, visit acamsglobal.org/virtual

ON THE COVER



How risky is your risk
assessment?

26

ACAMS Today 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 Bayview Center
80 Southwest 8th Street,
Suite 2350
Miami, FL 33130

Tel. 1-866-459-CAMS (2267)
or 1-305-373-0020
Fax 1-305-373-5229
or 1-305-373-7788
Email: info@acams.org
Web sites: www.ACAMS.org
www.ACAMSToday.org

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



ACAMSTODAY

ACAMS

John J. Byrne, CAMS

Executive Vice President

Karla Monterrosa-Yancey, CAMS

Editor-in-Chief

EDITORIAL AND DESIGN

Contributing Editor
Debbie Hitzeroth, CAMS

Graphic Design
Victoria Racine

SENIOR STAFF

Chief Executive Officer
Ted Weissberg, CAMS

Chief Financial Officer
Ari House, CAMS

**Global Director of
Conferences and Training**
Eva Bender

Head of Asia
Hue Dang, CAMS

Director of Sales
Geoffrey Fone

Director of Marketing
Kourtney McCarty

Director of Operations
Mike Vasquez

Head of Europe
Grahame White

SALES AND REGIONAL REPRESENTATIVES

**Senior Vice President of
Business Development**
Geoffrey Chunowitz, CAMS

Head of Caribbean
Denise Enriquez

Head of Latin America
Sonia Leon

**Head of Africa &
the Middle East**
Jose Victor Lewis

ADVISORY BOARD

Chairman:

Richard A. Small, CAMS
SVP-Enterprise Anti-Money
Laundering, Anti-Corruption
and International Regulatory
Compliance, American
Express, New York, NY, USA

Luciano J. Astorga, CAMS
Regional Chief Compliance
Officer, BAC|Credomatic
Network, Managua,
Nicaragua

Samar Baasiri, CAMS
Head of Compliance Unit,
BankMed, Lebanon

David Clark, CAMS
GE Capital, Financial Crime
Leader EMEA, The Ark,
London

Vasilios P. Chrisos, CAMS
Americas AML & Economic
Sanctions Director, Macquarie
Group, New York, NY, USA

William J. Fox
Managing Director,
Global Financial Crimes
Compliance Executive, Bank
of America Corporation,
Charlotte, NC, USA

Susan J. Galli, CAMS
Director of the Anti-Money
Laundering Strategic Planning
Office, HSBC North America,
New York, NY, USA

Peter Hazlewood

Global Head, Financial Crime
Risk Operations, Standard
Chartered Bank, London

William D. Langford

Global Head of Compliance
Architecture and Strategy,
Citi, New York, NY, USA

Karim Rajwani, CAMS

Vice-President, Chief Anti-
Money Laundering Officer,
Royal Bank of Canada,
Toronto, Ontario

Anthony Luis Rodriguez, CAMS, CPA

Global Compliance Officer,
Associated Foreign Exchange,
New York, NY, USA

Nancy Saur, CAMS, FICA

Compliance Manager
Millennium bcp Bank & Trust,
Cayman Islands

Markus E. Schulz

Chief Compliance Officer
EMEA, GE Capital, London, UK

Daniel Soto, CAMS

Chief Compliance Officer,
Ally Financial, Inc.,
Charlotte, NC, USA



- 6** From the editor
- 6** May–July CAMS Graduates
- 8** Member Spotlights
- 10** A message from the executive vice president
- 11** Kenneth Rijock: Author of *The Laundry Man*
- 12** Dennis Lormel, CAMS: Assessing the convergence between transnational criminal organizations and terrorist groups
- 14** Congratulations to the Greater Twin Cities Chapter! The 2013 Chapter of the Year Award recipient
- 16** A Bitcoin further down the road
- 18** Fraud analytics: Strategies and methods for detection and prevention
- 20** Redefining due diligence: A paradigm shift for AML/BSA compliance
- 22** Courage in compliance
- 26** How risky is your risk assessment?
- 30** Partners in anti-crime
–Law enforcement outreach enhances BSA/AML programs
- 34** Negative news –Discovering and verifying entity due diligence information
- 36** A deep dive into country risk assessment
- 40** Raise your voices: We hear you
- 42** Old MacDonald of sanctions compliance and customer due diligence
- 44** Mexico's security threat: Organized crime and money laundering
- 48** Canada 2013: The fight against financial crime continues
- 52** ACAMS releases findings of 2013 Compensation Survey: Median earnings for CAMS-certified professionals 32 percent higher than non-certified counterparts
- 54** ACAMS Risk Assessment: An in-depth look
- 58** The case for centralized KYC
- 62** Meet the ACAMS Staff



Risk — A four-letter word that we deal with daily. Assessing risk is part of everyone's life, whether it is during your commute to work passing the slow car in front of you, moving to another country and beginning anew, taking a job that can make or break your career, choosing to attend or not to attend an ACAMS' conference, bungee jumping off a bridge for fun or choosing a significant other. Life is full of risk. There is that old adage of no risk no reward. This holds true for many financial institutions and in turn makes the compliance department even more valuable.

This issue is all about risk. Here at the ACAMS editorial department we assessed our risk and decided that an issue focusing on the topic was worth pursuing.

Financial crime professionals deal with assessing risk on a daily basis. Let's face it: That is part of your job. The headline in the cover article starts by asking an important question that all compliance professionals should ask themselves: *How risky is your risk assessment?* The article goes beyond traditional risk assessment mechanics in favor of practical, actionable and easily implemented best practices. In a two-step process this article outlines how-to analyze and build a sound methodology for your risk assessment program.

Continuing with our risk theme, the second headline article *A deep dive into country risk assessment* discusses country risk assessments, which are key components for supporting the overarching risk assessment program and maintaining a sound sanctions program. Learn the three-step process that will help you maintain an effective country risk assessment program within your institution.


A Bitcoin further down the road follows the latest developments and challenges presented by virtual currencies, namely Bitcoin, and postulates next steps to be taken outside the U.S., by money launderers and compliance professionals.

Courage in compliance epitomizes the personal risk of a compliance professional and how her resilience helped law enforcement shut down the processing of illegal gambling activity within a bank. This article outlines lessons learned and the difference that one person can make.

This edition also contains highlights of the *2013 Compensation Survey* released by ACAMS in May and also an in-depth look and an interview with the key developers of the ACAMS Risk Assessment tool to be released later this year. For more info, please contact Tanya Montoya at tmontoya@acams.org.

Congratulations to our *Chapter of the Year* award recipient, Greater Twin Cities Chapter! *ACAMS Today* had the opportunity to interview two chapter board members about the chapter's accomplishments. Be sure to congratulate the Greater Twin Cities Chapter and also the other award recipients that will be announced at the *ACAMS 12 Annual AML & Financial Crime Conference* in Las Vegas.

Finally, we hope you are reading the *ACAMS Today* either in print, online (acamstoday.org) or via the *ACAMS Today* App. As always, please send any suggestions, comments or article submissions to me at editor@acams.org.

We hope you will take a risk this September and attend the *ACAMS 12 Annual AML & Financial Crime Conference*. We will see you there! 

Karla Monterrosa-Yancey, CAMS
editor-in-chief

May–July CAMS Graduates

Nadine Abdelnour
Khan Ahad
Sean Aitken
Adel Ahmed Abdulla Al-Mahmood
Mohammed Adnan Al Ansari
Abeer Faez Al Faez
Nafe Al Ghanmi
Hussam Al-Abed
Stephen Alexander
Kristine A. Allmendinger
Moh'd-Ali Bassam Mohammed Al-Nahar
Amal Mahmoud Ali Aham Al-Sheikh
Rania Alshelleh
Giuseppe Alvaro
Laith Zyad Jamal Al-Zubi
Maynor Augusto Ambrosio Higueros
Mohamed Nooral Amin Vellamadathil
Catherine Amundson
Tito Milan Andrada
Courtney Andren
Benjamin E. Anwuri
Laetitia Arrenault
Esperanza Arthur
Oren Brant Atchley
Chanthamaly Atkinson
Ali Faisal Baalawi
Berlin Babu
Kieron Bailey
Sherene Bailey
Janice M. Balber
Bryan Ball
Lauren Barrett
Ajwad Bataineh
Dolores D. Bedell
Mark Bennetts
Harvey Berger
David Betty
Massimo Bianchi
Kimberly Bischoff
Dianne Blais
Jonathan L. Block
Caroline Bomfim
Myfanwy P. Bonilla
Adelita Victoria Bonilla Idais
Lauren J. Bonney
Mosa Ahmad Boran
Solonggowa Borzigian
Toussant Boyce
Dedric Boyd
Scott J. Bradford
Matthew Brawner
Rebekah Broussard
Kaylan Brugh
Ning Bu
H.L. Buffington
Henry E. Bunting
Patrick H. Burns
Scott Burton
Sydney Buthelezi
Leavonne A. Campbell
Tara Campbell
Karla A. Campo
Harold Capshaw
Kimberly Ann Caras
Michael J. Carpenter



CAMS GRADUATES

Joy A. Carter
Stephanie Casanova
Pedro Jose Castillo Zepeda
Johnny X. Castro
Harold E. Cawley
Carolina Ceballos
Hellen Chandler
Jose Chavez De La Torre
Bonnie Cheung
Chik Yau Cheung
Wai-Ming Cheung
Raymond Seow Suan Chew
Dawn Chiam
Yi-Min Chien
Tong Chin
Miran Cho
Erica Cih
Elizabeth Coburn
Christina Collett
Molly J. Collins
Joseph Conniff
David B. Consigli
Kristin Coopman
Brandon Corchinski
Hector Galeon Cordero
Darren Cormier
Victoria Corral
James Costello
Tracy L. Coykendall
Cheryl Cravens
Pablo Cubi
Martin Cunningham
Julie Curto
Kendahl A. Cusimano
Jon Dale
Rabee Damra
Mutaz D'ana
Ana De Lima
Hilton De Paoli
Rose De Pinto
Carolina Ana Maria De Rooy
Ann M. Dean
Todd Deffenbaugh
Carol DeJoseph
Philip E. Delgado Smith
Kaan Demirel
Gladys Denegri
Bridgit M. Denz
Ronak S. Desai
Devakumar Sudha Devadas
Joel Diaz
Joseph DiLella
George Dimopoulos
Katherine M. Dorton
Sibley Douglas
Edward Doyle
Tracy Dragolich
Jeri Dresner
Lukasz Dukala
Michael Anderson Dunlop
Amanda J. Duray
Kevin Dwyer
Charrisse Dyer
Emmanuel Dzakru
Robert Eaton

John Edwards
Marta Ehlert
Bjorn Einarson
Alaeldin Elgizuli
Jeanette Eliopoulos
Stephen Engrassia
Jose Espada
Laura Espinoza
Regina Estanqueiro
Joseph Evans
Ryan Farelli
Khuzama Abdel Majid Favez Alrawashdeh
Chao Feng
Jeffrey Fischer
Jennifer Fisher
Darcy Fitzhenry
Jenna Fitzsimmons
Daniela Fiumara
Dickson William Fong Garcia
Leigh Forejt
Christine Ann Fountain
Michael Franceschini
Nathanlie Georges Francis
Leah A. Franta
Daniel Frechette
Connell Bernard Friel
Frank Fruithoff
Yuya Fujii
Shiro Fukuchi
Dan Gaik
Calogero Galipo
Richard Garrie
Carlos Garza
Devendra Gautam
Lei Ge
Marguerite Gendron
Connor Gerson
Phaedra Gijssbertha
James Gillespie
Heather Glendenning
Maria Goldstein
Erin Gorinski
Antonius Gorissen
James Graham
David Grant
Jennifer Grant
John Gray
Winfield L. Gray
Alan W. Greenfield
Jacquelyn J. Gregg
Scott D. Grimble
Tatyana Grinvald
Rob Grootaers
Martin W. Grum
Edgar R. Guerra
Paul J. Gullledge
Catherine Gyimah
Adnan Shareeda Habib
Kathi Hacking
Natasha M. Hagood
Jennifer Haines
Carol Aguada Hallberg
Ju Yop Ham
Laurance Mohammad Hamzeh
Sandy Han

Ramzi Hanna
Wade Hardie
Darryl Harper
Jeremy R. Haynes
Huiting He
Benjamin Heatley
Robert Heller
Adam Hermes
Susan Hess
Jacek Hetman
Paula Hewitt
Laurie Goodine Hill
John Hinton
Carissa Hofstede
Tamara Horsford
Karen L. Hsueh
Cho Chi Hu
Shan Hu
Rendong Huang
Peter Huenig
Yvonne Huerta
Siu Lun Hung
Clara Hurtado
Gunawan Husin
Mohammed Ibrahim
Maureen Iles
Paul A. Immerman
Vittoria Incandela
Keng Kou Ip
Shehnala Iqbal
Ruba Itani
Philip Jacobi
Ryan Jagdeo
Lynda Jammerman
Marta Janic
Mustafa Mahmoud Jaradat
Jonathan Jarvis
Aylin Jewell
Rajesh Kumar Jha
Sukhjot Jhutti
Luis Jimenez Lopez
Mark Vincent Marcelo Jocson
Byron Johnson
Stephanie Johnson
David Jones
Lester C. Joseph
Liudas Jurkonis
Emily Kajita
Vaibhav Kalra
Sumiko Kanazawa
Naoki Kaneko
Ramanathan Karuppiah
Elaine Kase
Aprajita Kaul
Dilek Sarsin Kaya
Yuliya Kazakevich
Talar Kazandjian-Tanashian
Holly Elizabeth Kazee
Jacki Keeley
Scott Kelley
Laura Kety
Jack Robert Khabbazian
Asif Alil Khan
Shuja G. Khan
Kristin Khoobyarian

Lucky Kihodu
Cody Kimura
Ben Koester
Lauren Kohr
Azusa Koike
Philippe Wong Kok Chin
Thomas W. Kolb
Philipp Koskinas
Andrew Michael Krajewski
Barbara Krekstein
Ibrahim Krishan
Stefanie Kronenberg
Alfreda Kulah-Samuel
Chia Heng Kuo
Jolanda Kuo
Nina Lacevic
Catherine Kar Ying Lam
Marianne Thi Lam
Keisha Lamy
Brian A. Lane
Tyler W. Langford
Joseph Lapczynski
Elizabeth A. Larson
Andy Chun Ho Lau
Tsui Heung Lau
Clare Lazenby
Anh Le
Kayla Le
Alice Lee
Roger Lee
Wontaek Lee
Joseph P. Leece
Nicole Lehman
Tirina Lehman
Tirina Lehman
Man I. Lei
Yew Joe Leong
Sylvia Lewis
Diana Lie
Chih-Chiang (Michael) Lin
David Litsky
Minxi Liu
Ye Liu
David Long
Michael Lowe
John H. Ludemann
Christophe Ludwig
Antonio Luk
Dannielle MacDonald
Marvin Madorsky
Pyotr Maghdashyan
LeAnne R. Magill
Colin Mai
Wing Chung Lena Mak
Julie Malec
Marie Andree Malo-Mongeau
Shujia Mao
Ronza Salameh Marji
Victoria Markosov
Todney Marsh
David Martin
Wilson Alejandro Martinez Sánchez
Tara Cooney Mata
Jonathon Matuszak
Brian Maynard

David McClanahan
David B. McCollam
Melissa A. McComas
Edward McCusker
Vanda McDonald
Stewart McGlynn
Karen McGuinness
William McManus
LaShonda McMorris
Chris McNaught
Frances Meany
Michael Melis
Robert Mensinger
Kirk Erwin Meyer
Joe Mikuni
Russell Miller
Susanna Mills
Brian Miloscia
Yap Ming Ying
Sandy Mirgon-Watkins
Christopher Mitcham
Mariusz Mlynarczyk
Nadia F. Mohammed
Zahid Ali Abdulla Mohammed
Beth A. Mohr
Norberto Molina-Perez
Lois Mae Molitoris
David R. Moore
Elizabeth Morgan
Karen Motley
Mirelle Moukarzel
Douglas Mourne
Angela Mueller
Lisa Saldana Muller
Pawel Muniak
Laura L. Murray
Nada Majed Musallam
Brett K. Myers
Shoba Nagaraj
Yongliang Nah
David Nahum
Shyamala Ajay Naik
Agnes Namoya
Claudia Narozny
Daniel Nash
Muhammad Shahid Naveed Bhatti
Wen Neo
Hari Kumar Nepal
Dilli Ram Neupane
Kimberley Ng
Khuong Thi Xuan Nguyen
Louise Nguyen
Brad Nichols
Teresa Norris
Jenna North
Stephanie North
Cathleen Norton
Jocelyn Norval
Farrukh Nuridinov
Jewell Nutter
Konrad Nyzio
Damian John O'Riordan
Chris Oehlert
Andrew Oh
Randy Oliver

Zachary C. Oliver
Anna Ono
Chiazor Onwuegbuzie
Benson Pui Chung Or
Stephen Orubor
Adetutu Oshineye
Masanori Ota
Debbie Owens
Christine Park
Kwonsik Park
Laura Paterson
Tiffany Patrick
Jaroszewicz Pawel
Chandi S. Perera
Christina Peri
Rudolph Persaud
Samcy Philip
Karen S. Phillips
Khushal Phullah
Amanda Jessica Piccone
Gwen Pineau
Tony Pleasant
Qiu Wen Poh
Herbert Pontzer
Angela Poulin
Kerri L. Provenza
Muaadh Mohammed Saeed Qasem
Liu Yong Quek
Gabriel Quispe
Michael C. Rakower
Candice Ramlogan
Jonathan Ramos
Selma Ranghamar
Pamela Ranneby
Redeesh Trivikrama Rao
Shadee A. Rasul
Stephen R. Rayo
Zeeshan Raza
Vidya Reddy

Shannon Reed
Kevin Reese
Doede Martijn Rensema
Davin K. Ripley
Jessica Rodgers
Minerva Roman
Wendy Rosner
Matthew Rothstein
Matt Rotter
Christopher Rowland
John P. Ruedinger
Elda Ruiz
Jorge Othon Ruiz Hernández
Brooke A. Runk
Christopher Russo
Giselle Ryan
William M. Ryan
Ganeshkumar S.
Nesreen Abd Al-Qader Saadeeldeen
Ismail Salameh
Ashraf Muhi Eddin Samhour
Jessica Lynn Sammut
Sophie Sanders
Claire Sarzynski E.
Meenal Sathe
Mark Satterfield
Jesus Saucillo
Alison Scalvini
David A. Schechter
Karen S. Schellin
Marc Schindelheim
Lynnette Schroedel
Marvin Keith Schroeder
Ashley Scott
Lesley J. Scott
Sean Seaborn
William F. Seaward
Arnab Sensarma
Raul Serrano-Diaz

Atif Shaikh
An Teresa Shan
Scott David Shapiro
Kartavya Sharma
Christina Odeh Shemali
Derek Shepherd
Jordan B. Shepherdson
Kathleen Sherban
Damian Sikorski
Laura Silver
Lauren Silver
Shannon M. Simmons
Hardeep Singh
Bobbie Smith
Ewart Smith
Luz Marina Smith
Michael Smith
Travis Charles Smith
Wayne Smith
Beverley Smyk
Kamal Soni
Todd Spicer
Maciej Spiewak
James Steiner
Stanley Stern
Daniel Stitt Jr.
Lisa Stokes
Fredrik Strand
Ronald J. Strzelecki
Ahmed H. Sukar
Brett James Sullivan
Jennifer Sun
Jennifer M. Surace
Delores J. Swires
Anna Talbott
Hui Ling Tan
Tingting Tang
Denise Dion Tansey
Ahmad Tarteer

Ashley Tassell
Johnny Teng
Dennis Thornbloom
Mayra Tijerino
Conrad Tillett
Carmen Tong
Irene Torres
Prakash Totala
Mohammed M. A. H. Toukan
Miriam Tovar
Krystian Trybus
Hiu Kin Tse
Jessica Turnbull
Kiyonobu Ueda
Amber Unick
Meenaz Ahmad Vaidya
Hannes Valtonen
Rene Armand Van Zessen
Lucille Vaughan
Teresita Velazquez
Travis Vermeulen
Adrian Vicente
Krishnan Viswanathan
Jeffrey Walk
Kristin Walle
Thomas Xiang Wan
Jamie Wang
Ruohan Wang
Yan Wang
Georgina Ward
Greg Ward
Sharon Ward
Marcin Wasilewski
Barbara Wastle
Cori M. Wells
William Westington
Michael Wikison
Barry Williams
Dave Williams

Mark Williams
Pamela L. Williams
Valerie Williams
Debra Williams-D'Arrigo
James Winkler
Michael Winter
Anne Therese Witkowski
Hiuyin Wong
James J. Wood
Kyle Wright
Nicole Wright
Julianna Wu
Steven Z. Wu
Tigist Wubru
Kristina Wyatt
Osamu Yamanaka
Elaine Yancey
Allen Yao
Basil Yeung
Shing Kam Yip
Erik Yoder
Golrokh Youshidje
Ahmad Tawfiq Younes Tawfiq
Samantha Young
Ai Zhen Yu
Henry Yu
Vincent Yuen
Roger Abou Zeid
Tao Zeng
Christine Zenzerovic
Naiwen Zhang
Qian Zhang
Qiling Zhang
Rongliang Zhang
Xiaohui Zheng
Rawand Ziad Turk
Jacqueline Ziemniak
Nicholas Zigelboym

Member spotlights



Carolina Ceballos, CAMS
Paris, France

Carolina Ceballos has more than six years of experience in the banking and insurance industry as a compliance and money laundering expert. She holds a master's degree in business law with a strong emphasis on anti-money laundering and counter terrorist financing (AML/CTF).

For the past several years, Ceballos has worked for the French Supervisory Authority (ACP) in both the banking and the insurance sectors. In her current role as an AML/CTF senior auditor, she leads off-site investigations and ensures that institutions meet their due diligence and FIU reporting obligations. She participates in the

development of the AML audit methodology and trains new investigators on auditing techniques and practices, financial sector and AML/CTF regulations.

Prior to joining the ACP, Ceballos served as a compliance officer in major banking institutions. She was in charge of the due diligence investigative process, the collection and retention of compliance records and suspicious activity reporting.

Ceballos is a subject-matter expert in European and French banking laws, rules and regulations, audit and examination codes and guidelines for best practice techniques concerning AML, know your customer (KYC)/enhanced due diligence (EDD), training, record keeping, sanctions screening and suspicious activity recognition and reporting.

She participates in FATF, World Bank training sessions and is an AML/CTF lecturer at the University of Strasbourg.



Reindorf Atta Gyamena, CAMS
Accra, Ghana

Reindorf Gyamena has over eight years of experience in the financial services industry. He is currently the head of compliance at CAL Bank Ltd where he oversees the bank's entire compliance function. Prior to this position, he was the head of market risk unit at Intercontinental Bank Ghana Ltd. Before joining the banking sector, he worked as an audit assistant at Aryitey & Associates, a private Chartered Accounting firm in Accra, Ghana.

He holds bachelor degrees in Economics and Political Science from the University of Ghana — Legon. He is a chartered banker and associate member of the Chartered Institute of Bankers (Ghana). He is also a Certified Anti-Money Laundering Specialist (CAMS).

He has attended several international and local courses on risk management, treasury function, auditing, fraud, anti-money laundering and combating financing of terrorism, financial crimes prevention, and Basel II framework.

Gyamena has served as a resource person and speaker at both local and international conferences, training and workshops on AML/CTF and financial crimes, including ACAMS Africa Conferences.

He conducts AML/CTF training for staff of CAL Bank and administers the bank's AML/CTF e-learning program where he prepares all study materials and test questions. He also offers consultancy on the establishment of compliance and the risk management function, drafting AML/CTF program, drafting and revision of customer due diligence/know your customer (CDD/KYC) policies for financial institutions.

Gyamena has been instrumental in the formation of compliance officers' forum of banks in Ghana and provided valuable contribution to Ghana's Financial Intelligence Centre (FIC) in the introduction of Currency Transaction Report (CTR) regime in Ghana. Currently, he is leading a team of dedicated ACAMS members in Ghana to form an ACAMS local chapter in Ghana.

With his strong commitment to the fight against money laundering and terrorism financing in Ghana, he was selected by Ghana's FIC as part of a three member delegation to represent Ghana at GIABA's AML/CTF seminar/workshop in Dakar Senegal in 2011, where he made valuable inputs into the communiqué that was issued after the conference.



Rosalind Laruccia, CAMS, LLB
Toronto, Canada

Rosalind Laruccia is a senior manager with RBC Global AML Compliance, managing the Global Sanctions Group. She has 13 years of experience in risk management, internal audit, AML and corporate compliance in Canada, the U.S., and the E.U. in both the telecommunications and financial services industry. Laruccia's roles have included investigations, auditing, risk management and control, training, money

laundering/counter-terrorism financing and global economic sanctions.

At RBC, Laruccia provides global economic sanctions guidance across the bank, in addition to utilizing her audit knowledge in assisting the AML compliance group with policy and other control related activities. As senior manager she is responsible for the development and implementation of a consistent global economic sanctions program that includes payments escalations, development of key documentation, sanctions investigations, as well as to ensure the bank's compliance with sanctions requirements within the jurisdictions that RBC operates.

As the ACAMS Greater Toronto Chapter executive secretary, Laruccia organizes and drives the chapter's events, conferences and manages their LinkedIn group ACAMS Canada page. In addition, she works with her other chapter board members to bring AML training and discussions to various AML professionals in Toronto and the surrounding areas.



Sylvain Perreault, CAMS
Montréal, Canada

Sylvain Perreault is currently the chief compliance officer of Desjardins Group, the largest financial cooperative group in Canada with \$200 billion of assets under management. He manages a group of 180 compliance professionals, 35 of them are part of the anti-money laundering (AML) team.

The AML team is currently working on setting up and establishing parameters for a new software tool. In addition, a new online course was launched in 2013 which will benefit close to 20,000 employees working in the branch network. It is a great tool for underlining the importance of identifying and reporting suspicious activities.

Perreault is also currently involved in the September 2013 launch of an ACAMS Montreal Chapter. An initial networking event was held on May 23, 2013. The event was a great success and 118 people attended. With the recent launch of a Vancouver Chapter and the Montreal Chapter soon to launch ACAMS is rapidly expanding in Canada.

Prior to his appointment at Desjardins Group, Perreault also worked in the securities business, initially for the Montreal Exchange where he held several positions including SVP of Markets. He also founded a brokerage house in

2001 and acted as CCO and COO of Desjardins Securities a subsidiary of Desjardins Group.

Perreault also has extensive international experience. He was involved in the 90s launch of a stock exchange and clearing house in West Africa (Abidjan) and a dealers market in Cameroon. He currently serves on the board of the Investment Industry Association of Canada (IIAC) and the Special Regulation Committee of the Montréal Exchange, a subsidiary of TMX Group.




Samah Fadhil Sukkar
Amman, Jordan

Samah Fadhil Sukkar is the head of compliance of Alrowad Exchange and has been with the company for six years. Alrowad Exchange is one of the leading companies to intermediate the selling and purchasing of foreign currencies and transfers in Jordan and Iraq. Sukkar has extensive experience in understanding and dealing with international anti-money laundering laws, day-to-day trading correspondences, financial and technical negotiations, and order processes, money transfers and being the coordinator and organizer between the parties of financial institutions.

In addition, she has development and innovation experience in the compliance field. She has helped put together a group of AML/CTF specialists in the financial sector in Jordan to help in the fight against money laundering and terrorist financing. She was also instrumental in helping ACAMS partner with Iraqna Business training services and helped obtain approval from the Central Bank of Iraq to hold trainings and to establish an exam center where the CAMS exam would be available for the financial sector in Iraq.

She contributed as an AML advisor at the Federation of Iraqi Private Banks and held training for Iraqi employees of money transfer companies in Iraq Erbil.

Sukkar attended the *18th Annual International Financial Crime* conference in Hollywood, Florida and the 2013 MENAFATF conference in Dubai. In addition, she participated in a loan conference held in Baghdad which was sponsored by the Central Bank of Iraq in 2013, a seminar held in IBS about AML/CTF in Jordan and a 2013 national anti-corruption campaign in Iraq with UNDP Iraq.

Sukkar holds a bachelor's degree in Engineering from the Baghdad University. 



Get active and share!

I just returned from my college reunion (no, I won't say which year) and it is at times like these that I am reminded how fortunate we all are to be in the anti-money laundering (AML) community. Explaining to others what field you are in can be daunting, because some are so quick to judge, but I am constantly pleased at the interest we get from others for the work we have chosen — or in some cases were thrust into by happenstance.

People seem genuinely interested in a profession where the goal is to deter, detect and report money laundering — a crime we all know is connected to a vast array of criminal activity. While we sometimes struggle with compliance and legal obligations, there is no denying that the three parts of AML: Law enforcement, regulators and the private sector are all committed to the same goal. As we head toward the *ACAMS 12th Annual AML and Financial Crime Conference*, it is a good time to reflect on the good work of our community and to be proud of our successes. ACAMS is honored to represent all facets of this august group.

Risk assessment — A new offering to our members

Since this edition has extensive coverage of the risk assessment challenges for financial institutions, I will just add that ACAMS has been diligently producing the ACAMS Risk Assessment tool with a committee of experts since December 2011 and we will be releasing the product following the

Vegas conference. We are very excited at the opportunity to create clear AML community standards and enhance the financial sector's ability to risk rank, add appropriate controls and provide regulatory transparency on risk assessment methodologies.

ACAMS continues to address the global AML/Financial Crime community


Hopefully you follow the progress of your association and all of our members through your local chapter, the web sites and mobile applications we offer. As you do, you will quickly realize that while all of the ACAMS staff works as a team, ACAMS has staff dedicated to different regions of the world so the membership has a "go to" liaison for all jurisdictions. In addition to Hue Dang, the long time head of Asia, ACAMS has been fortunate in the past year to expand its staff responsible for the various regions to include Grahame White as head of Europe, Jose Lewis as head of Africa and the Middle East, Sonia Leon as head of Latin America, Denise Enriquez as head of Caribbean and we have always had David Kehr as our key contact with law enforcement in North America and elsewhere. I urge you to find out who your main contact is and to take advantage of them as a resource.

There is no question that ACAMS is THE global organization dedicated to AML/Financial Crime professionals in both the private and public sectors. We are here and the leading organization because of you — our members!

Social media

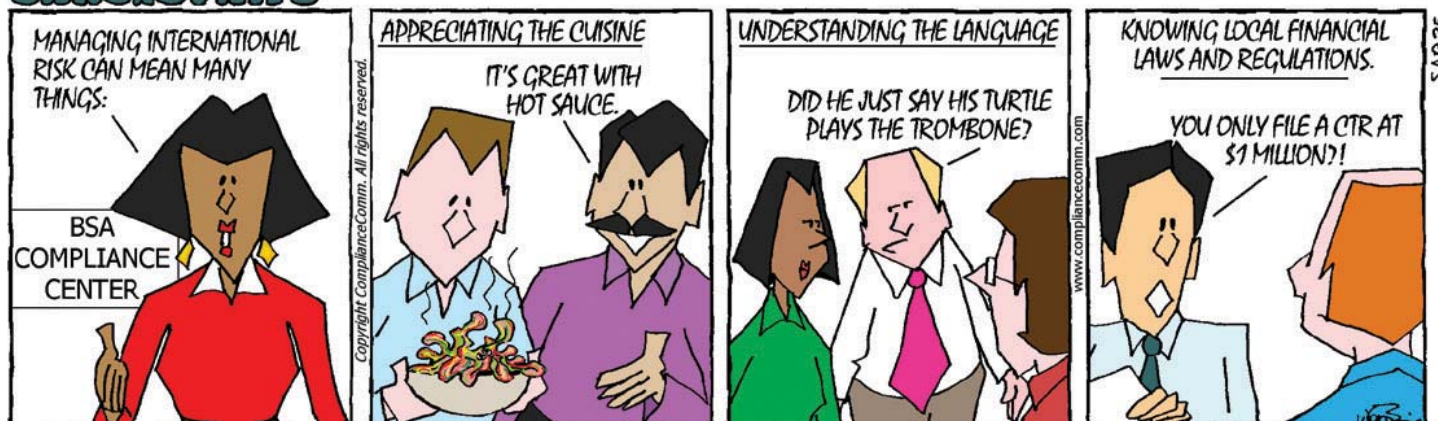
Conference season is a great time for delegates to share information with peers and offer recommendations on how to stay informed. The more traditional methods are encountered during networking at the conference, at sessions designed for information sharing and speaking one-on-one with other attendees. As many conference organizers always stress — leave with contacts, business cards and some questions answered or your attendance is not complete.

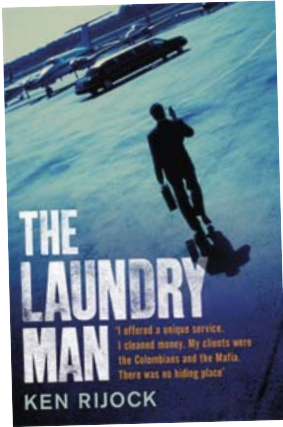
The past several years have seen the growth of technologies that enhance information sharing. Whether it is immediate response mobile phone (or other application) surveys, Twitter or the many other forms of social media, the opportunities for information compilation appear limitless. ACAMS has three Twitter feeds at this point with more to be added. Please let us know what else we can do to continue to keep you informed and follow me (@jbacams2011), Kieran Beer (@KieranBeer) and ACAMS (@ACAMS_AML) on Twitter or Facebook (Association of Certified Anti-Money Laundering Specialists) or the various ACAMS chapter channels.

There is no excuse for not connecting in 2013! 

John J. Byrne, CAMS
executive vice president

SARSENSTRIPS™





Kenneth Rijock: Author of *The Laundry Man*

Robert Goldfinger had the opportunity to speak with Miami financial crime consultant Kenneth Rijock, whose first-person story, *The Laundry Man* details his decade as a career money launderer.

Robert Goldfinger: In your book, *The Laundry Man*, you give a fascinating account of your journey from successful lawyer to money launderer, then transitioning back to the “good guy.” Share with me what enticed you to go down the path of criminal activities?

Kenneth Rijock: It was a perfect storm; the combination of a difficult home situation ending in my divorce, with no children, and entering a new social circle that included several fellow Vietnam veterans, all of whom shared my 1960s perspective on the position that personal drug use should not be criminalized. When I discovered that my new friends were not exactly whom they appeared to be, the fact that they were involved in drug smuggling did not deter me, as this was free-wheeling Miami in the 1980s. I then believed in decriminalization, but my experiences since have caused me to presently support the anti-drug laws.

RG: As detailed in the book most, if not all, of your criminal activities took place in South Florida and the Caribbean. Why was that geographical area a prime venue for your criminal activities, and to the best of your knowledge, how has that changed?

KR: At that time, Florida was in the epicenter of the narcotics trafficking world in North America, as well as the location of much of the money laundering, and bulk cash smuggling. I did not have to go far to find cooperative offshore tax havens, where they asked no questions about source of funds, and beneficial ownership of companies that I was forming, through local counsel. Though today it is not as overt, Caribbean tax havens continue to facilitate massive amounts of drug money laundering.

RG: You mentioned in the book that you came from a humble immigrant background. Did your immigrant family experience work as a compass to guide you out of criminal activity or was there another catalyst?

KR: The major influences, those individuals who I believe brought me back from a dark place, were not my conservative family, but a United States Marshal and a police Sergeant from Florida, who showed me that I needed to be part of the solution, and not part of the problem when it came to money laundering. Their confidence in me guided me back to the light.

RG: It is obvious that your time in prison was not a pleasant experience. Prison sentences are becoming more frequent for financial crime convictions. Do you think this has an impact on criminal behavior or the decision to become involved in criminal activity?

KR: Unfortunately, most financial criminals never consider the possibility that they may one day be convicted of a felony. Most think that their scam is too good to be identified, so they do not fear arrest. This is called denial and it ignores reality. The respective 50 and 150 year sentences meted out to Scott Rothstein and Bernard Madoff, the two biggest Ponzi schemers, will not deter others in my humble opinion, for successful fraudsters are generally far too arrogant to take the risk of arrest seriously.

RG: In your activities you moved a lot of cash. Has technology changed the methods?

KR: Yes, though bulk cash smuggling, where money launderers move the proceeds of crime into a cooperating offshore jurisdiction, the rise of technology has opened many new targets of opportunity through which laundrymen can successfully complete their illegal missions, including international trade, virtual currency, online creation of corporations, and the expansion of tax haven products and services. All which have moved money laundering forward and decreased the risk of identification, interdiction and arrest. Money laundering is more efficient now and easier to accomplish, unfortunately.

RG: What advice do you have for a lawyer or compliance officer that may be considering improper or illegal activities?

KR: Ladies and gentlemen: All the money and adult toys in the world are not worth the consequences of arrest, conviction, and incarceration, especially for a professional, for he or she will not be able to return to their previous life after their incarceration is completed. They will

be forever stigmatized and find that the path to legitimacy is a long, hard road, with many obstacles in their way. Your reputation is priceless, and once lost can rarely be restored.

RG: In the book, you chronicle the years-long criminal investigation conducted by law enforcement. What was it like to live under that uncertain cloud?

KR: The daily pressure was intense, and it continued even when I was off duty, for one never knew when the proverbial “knock on the door” would come, as you always knew it would. I found the stress similar to that which I experienced while serving in the U.S. Army in Vietnam and Cambodia during the war; a dull pain, or feeling in the back of your mind that there was trouble headed your way, and that your future was not bright.

RG: What are five “bits of wisdom” that you would like to share with those of us in the financial crimes prevention community?

KR: (1) Money launderers are as educated, as smart as, and more innovative than you are; they often speak more languages, and have previously been bankers and lawyers. Do not underestimate them.

(2) Good money launderers are forever looking for weaknesses in your bank’s compliance program, and when they find one, they drive a truck through it and successfully move illicit funds. Keep updating your program. Pick up new software and commercial database resources that will be useful tools.

(3) Do not neglect your in-house AML/CTF training program. Often, only senior compliance staff is sent to seminars and conferences; send your junior frontline staff as well.

(4) Make sure that you periodically check your most valuable and successful bank customers, lest they turn out to be Ponzi schemes whose operation was overlooked by enthusiastic customer relationship managers.

(5) Above all, regard compliance as a challenge and an adventure, as I did when I served in that capacity; use your imagination, because rest assured that your money laundering opponents are staying up nights and weekends creating schemes to move money through your bank. **FA**

Interviewed by: Robert Goldfinger, CAMS, CFS Cmdr. CID (retired), president, Nomino Data, USA, rgoldfinger@nominodata.com



DENNIS LORMEL, CAMS:

Assessing the convergence between transnational criminal organizations and terrorist groups

A *CAMS Today* spoke with Dennis M. Lormel the founder and president of DML Associates, LLC about the convergence of transnational criminal organizations and terrorists.

Lormel and associates provide consulting services and training related to terrorist financing, money laundering, fraud, financial crimes and due diligence. For 28 years, he served as a special agent in the FBI and served as chief of the FBI Financial Crimes Program. There, he formulated, established and directed the FBI's terrorist financing initiative following the terrorist attacks of September 11, 2001.

For his visionary contributions, Lormel received numerous commendations and awards to include the Department of Justice, Criminal Division's Award for Investigative Initiative and the Central Intelligence Agency's George H. W. Bush Award for Excellence in Counterterrorism.

ACAMS Today: What are the commonalities between transnational criminal organizations and terrorists?

Dennis Lormel: Transnational criminal organizations and terrorist groups share many operational and organizational similarities and characteristics. They often learn from one another, imitate each other's successes and failures, and frequently partner with each other. There has been an evolution wherein these groups have developed into hybrid criminal/terrorist entities. As a result, the nexus between transnational criminal organizations and terrorism has become increasingly complex and sophisticated.

AT: Is the convergence of transnational criminal organizations and terrorists on the rise and if so why?

DL: Transnational criminal organizations and terrorist groups have increasingly found common ground of mutual benefit. Each has learned how to benefit from conflict. The

Terrorists have had to engage in criminal activity, particularly drug trafficking, to fund themselves

Arab spring and conflicts in Africa and other places have created opportunities for criminals and terrorists to exploit the weaknesses of the states in conflict. These entities have also benefited from their convergence with each other and from their ability to diversify their activities through licit and illicit mechanisms.

One of the primary reasons why the convergence of transnational criminal organizations and terrorist groups has been growing is that legitimate funding sources that terrorists relied on have dried up. For instance, al-Qaeda and related groups traditionally relied on wealthy donors for funding. As the U.S. and friendly countries exerted pressure through sanctions and other actions, wealthy donors stopped providing funds. Likewise, Hezbollah traditionally relied on funding from state sponsors Iran and Syria. Those funding sources have diminished considerably. Consequently, terrorists have had to engage in criminal activity, particularly drug trafficking, to fund themselves. They learned quickly how valuable and enriching collaborating with criminals could be.

AT: Which types of organized groups are more inclined to collaborate with terrorists and why is understanding this linkage important for a financial crime prevention professional?

DL: Longstanding transnational organized crime groups and newer crime groups have very different relationships with terrorism. Traditional organized crime groups like the Italian and Russian mafia, and Asian organized crime possess long term financial strategies. They are dependent on long established states where they operate in. They tend to reject associations with terrorism. Importantly, they have different strategies and motivation which are not conducive to collaboration with terrorists.

Newer criminal groups do not possess long term and efficient financial strategies. Groups like the Haqqani network in Afghanistan, D-Company in Pakistan and Los Zetas in Mexico, operate and thrive in ungovernable regions. They take advantage of chaos and dysfunctional states. These groups generate huge profits from cooperating with terrorists. They have more consistent interests with terrorists that are conducive to collaboration.

AT: Can you give us an example of an actual case you have worked on where you saw this type of collaboration?

DL: The best example of this collaboration can be found by assessing the Lebanese Canadian Bank case. It was an elaborate international drug trafficking and trade-based money laundering operation involving the Joumma drug trafficking and criminal organization in Lebanon, Los Zetas drug cartel in

Mexico and Hezbollah, the Lebanese based terrorist organization. This collaborative criminal enterprise laundered approximately US\$200,000,000 per week. The Lebanese Canadian Bank wired over US\$329,000,000 through the United States. Most of the funds were intended to purchase used cars in the United States that were shipped to West Africa. Some of the funds were wired from the United States to Asia, where they were used to purchase goods that were subsequently shipped to Colombia. There was a particularly close and mutually beneficial

The Joummas, Los Zetas and Hezbollah profited greatly by collaborating together

nexus between the Joumma organization and Hezbollah since they both operate out of Lebanon. This was a truly global operation. The Joummas, Los Zetas and Hezbollah profited greatly by collaborating together.

This case exemplifies how two newer transnational criminal organizations found common ground with one of the most financially successful terrorist organization. Each made considerable money from working together to further their individual organizational interests. They used a variety of facilitation tools to include correspondent accounts, wire transfers and shell companies. This case demonstrates how convergence, coupled with the diversification of activities, present new challenges for law enforcement and the financial services sector.

AT: What steps can a financial crime prevention professional take to stay ahead of this new trend?

DL: The public and private sector must develop new methodologies and strategies to deal with the problem of convergence between criminal and terrorist organizations. Understanding the crime/terrorist nexus is the first step toward solving the problem. For instance, understanding what motivates groups to interact, which groups are more inclined to interact, how they interact and how they raise, move, store and access funds is critically important. By understanding these elements, strategies can be developed to disrupt the flow of funds; which leads to one of the main vulnerabilities of these types of organizations, finance.

AT: What type of training should financial institutions give their staff to prepare them to face this new financial crime trend?

DL: Training is an important component for dealing with this emerging problem. Financial institutions should implement training on two levels. First would be high level training to deal with the problem in a broad sense. The training should be geared to promote awareness that the convergence of transnational criminal organizations and terrorist groups is a growing problem that presents law enforcement and the financial services sector with new challenges. It should highlight why groups interact, who is more likely to interact, how, what criminal activity they deal in, what regions they conduct business in, what facilitation tools they use and how they are likely to use financial institutions. It should be provided to a wider group of employees within an institution. The second level of training should be more granular. It should focus on areas of risk that are institution specific. The training should include case studies that demonstrate how financial institutions can be exploited by criminals and terrorists working in conjunction with each other. The case studies should demonstrate how the institution was used. Finally, the training should promote proactive and targeted investigative techniques that could be used to detect, report and deter such activity from occurring at the financial institution. This training should be targeted to specific employees, such as fraud investigators, AML specialists and even include select business components. **▲**

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

Congratulations to the Greater Twin Cities Chapter!

The 2013 Chapter of the Year Award recipient

The ACAMS Greater Twin Cities Chapter was launched on October 27, 2011, by an executive board composed of professionals from the AML field in the Minnesota/Wisconsin region and has a membership of 60. The chapter's mission is to be a professional resource that can provide support, guidance, training and peer interaction for industry professionals.

ACAMS Today had the opportunity to speak with the chapter co-chair Jennifer Sosniecki from Allianz Life Insurance Company of North America and co-programming director, Sande Bayer from US Bank.

ACAMS Today: How did you first become involved with the chapter?

Jennifer Sosniecki: In 2011, ACAMS solicited interest from local ACAMS members on the launch of a new Greater Twin Cities (GTC) chapter. I raised my hand! A couple months later, I joined the executive board as

secretary and the GTC launched in October 2011. In 2012, the co-chair position opened up and I transitioned to that role. What I like best about our chapter is that our board members represent more than just the banking sector. We represent securities, insurance, retail and consulting. As we have a broader range of experience, I believe this has helped us draw in new members from different industries.

Sande Bayer: I attended a learning event by the Carolina's Chapter and introduced myself to John Byrne and asked why there wasn't a Twin Cities/MN Chapter. It wasn't long after our conversation that Kiren Schulte (the chapter chair) had been appointed chapter representative and everything started to fit together. We had a strong cross section of backgrounds from our board members and everyone was energetic about working together to have a successful launch. I still have that energy! After the first several

months, our board experienced vacancies because two members had job transitions. That allowed us to re-evaluate the board roles and responsibilities to best fit our skills, talents and specific market attributes. I love that flexibility, and that I am now able to be part of the events/programming team. Some may argue, but I think I have the best role on the board!

AT: What is the main obstacle faced by financial crime prevention professionals in the Greater Twin Cities area?

JS: Our chapter members are telling us they want more engagement from local law enforcement in communicating new financial crime trends. We all want to assist local law enforcement and prevent crime; however, we need to know what to look for! We hope to organize more events with law enforcement in 2014.

SB: Perhaps the biggest obstacle is breaking through the silos and establishing communication channels. Not only within some of our organizations, but also with local law enforcement. I'd like to see us all become more aware of the local and regional activity and trends our law enforcement is seeing and how different that is from the national and global information we receive. And then, translate those needs into how each of us in our varied roles and institutions can have positive input and build positive working partnerships against financial crime.

AT: Why is it important for ACAMS members to belong to their local chapters?

JS: With the current economy and companies cutting budgets, joining a local chapter can be a cost-effective way to continue your AML



Jennie Sosniecki provides opening remarks at the 5/22/2012 learning event "Minnesota Trends in Money Laundering and Terrorist Financing."



Top Row – Jennie Sosniecki, CAMS, Matt Johnson, CAMS, Michael Moore, CAMS, Ryan Montgomery, Tim Charbonneau, James Cummins, CAMS, Kiren Schulte, CAMS,
Bottom Row – Jen McGarry, CAMS, Jessica Baglo, Kami Belchak, Sandra (Sande) Bayer, CAMS.

education. In addition, local chapters offer great networking opportunities with other AML professionals.

SB: At first I thought the networking available through the chapter was the most important and appealing benefit. But now, as budgets are constrained and a good percentage of our members aren't able to attend national conferences, the learning events are critical. Our board takes this responsibility seriously and works together to have strong and successful events that feed and support our membership and attendees.

AT: Which chapter events are you most looking forward to attending this year?

JS: Our chapter is in discussions with a local fraud prevention association to partner on a learning event this fall. The topic will include how AML and fraud teams can work together and share best practices. Many of us already work closely with the fraud investigation groups in our organizations and understand the alignment between AML and fraud prevention. I think this will be a great topic!

SB: The ones our members ask for! When we choose to plan events around topics and speakers that the members ask for, those are the best attended and most engaging. We've got a couple ideas taking shape. One would be a follow-up to an event we did on human trafficking. In addition, the ever present regulators responsible for our members' diverse financial sectors seem to provide ongoing



Attendees at a learning event include AML professionals, regulators and law enforcement.

material for events. We always love to hear cases from our local law enforcement and how involvement from the AML community assisted in the cases. And then there's the world of innovations ... virtual currencies, mobile banking and the challenge of keeping up when our systems may not be as capable and up-to-date. Looks like we'll have another busy year!

AT: What do you hope to accomplish as a chapter board for 2014?

JS: Of course, we are like other chapters and want to increase our membership. In an effort to get there, we must find new and interesting topics for future events to keep the engagement of the local AML community. Our continued partnership with local law enforcement agencies and other industry groups in 2014 will be very important.

SB: As Jennifer stated, we'd like to increase our membership, and cast the net wider to include smaller FTs and more law enforcement. Our members are great! And when we listen to what they like about learning events for topics, location, timing, value, etc. those become our most successful events! I'd like to think that we can provide diverse topics, be innovative in location/presentation and partnerships and keep the passion fueled for our careers. It can be a challenge to re-visit topics like human trafficking or keep fresh content with events on regulatory requirements. Also, we want to look for more out-of-the-box events for this group! I'd like for all of our members to feel value and support from ACAMS and the chapter. **A**

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



A Bitcoin further down the road

The world of virtual currencies has been changing at Internet speed over the last six months, since *ACAMS Today* published an article about Bitcoin and the implications for anti-money laundering compliance in its March–May 2013 issue.

The catalysts

While the previous *ACAMS Today* article was being written, the European Central Bank (ECB) was busy issuing a report examining the current and future potential impact of virtual currencies on national economies, regulators and consumers.¹ The ECB report, in addition to categorizing the different types of virtual currency, profiles the two most prominent virtual currencies, Bitcoin and Linden Dollars.

Perhaps the most notable part of the report, however, is its final sentence:

Given that the current assessment of risks is highly dependent on relatively small-sized virtual currency schemes, the assumption that virtual currency schemes will continue to grow means that a periodical examination of the developments is needed in order to reassess the risks.

This statement is both a confirmation of one of conclusions of the previous article in *ACAMS Today*, as well as a call to arms to maintain vigilance before any impact of virtual currency economies on traditional national economies spirals beyond the ability of regulators to exert effective control, should the need arise.

Then, within weeks after the publication of the previous article about Bitcoin in *ACAMS Today*, the U.S. Department of Treasury's Financial Crime Enforcement Network (FinCEN) issued regulatory guidance on

applying AML regulations to those who use, administer or exchange virtual currencies,² noting in the very first paragraph:

A user of virtual currency is not an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations.

The consequences

The impact of FinCEN's guidance on Bitcoin was swift and dramatic. The price of the currency spiked to a peak of approximately US\$266 per coin (in contrast to the US\$15 price quoted in *ACAMS Today* and US\$30 price at the time of publication). The price ultimately collapsed to about US\$105 soon after due to system problems with Mt. Gox, the largest Bitcoin currency exchange, related to its inability to keep up with the trading volume. However, as this article is being written, the price is still around US\$95, or over three times the price less than six months earlier. Why the price remains at an elevated level remains unclear. It is a likely due to a combination of greater visibility of the virtual currency, the allure of its anonymity features and the attraction of something vaguely illicit, if not illegal.

U.S. regulators, meanwhile, practiced what they preached. In May, the Department of Homeland Security seized Mt. Gox's account with the Dwolla payment service³ because the exchange company had failed to register with FinCEN as a money services business (MSB).⁴

Less than two weeks later, Liberty Reserve, a Costa Rica-based virtual currency network, was seized and its owners were indicted for helping its over 200,000 users launder over US\$6 billion during its seven year history.⁵ Like Bitcoin, Liberty Reserve's allure was the anonymity of its users and transactions.

Most radically, at the end of July, the Bank of Thailand made the purchase, sale and use of Bitcoins illegal.⁶

For every action, however, there is an equal and opposite reaction. Toward the end of June, Mt. Gox registered as an MSB with FinCEN.⁷ As news of this got out, it caused some flight from Bitcoins, as the price dipped from over US\$100 per coin to about US\$70 in the two weeks after the registration. The price has stabilized since this drop.⁸ It is likely that having Mt. Gox's dollar transactions, which, according to the firm's web site, comprises 80 percent of Bitcoin trade, subject to the prying eyes of U.S. regulators made the currency less valuable to both currency speculators and potential users drawn by the anonymity of the Bitcoin blockchain.

In addition, at the end of July, Finextra reported that a number of virtual currency operators, including BitPay, Hub Culture and Yoyocard, have been discussing creating a self-regulatory body called Digital Asset Transfer Authority (Data).⁹ The group's stated goals are "promote the prudent, responsible development of emerging payment networks, establish common rules to protect users, and work as a liaison among businesses, customers and public officials."

¹ "Virtual Currency Schemes", *European Central Bank*, October 2012, 24 July 2013 <<http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>

² "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", *Financial Crimes Enforcement Network*, 18 March 2013, 24 July 2013 <http://finccen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf>

³ "Dwolla", *Dwolla*, n.d., July 24, 2013 <<https://www.dwolla.com/>>

⁴ Kashmir Hill, "The Feds Are Cracking Down On Mt. Gox (Not On Bitcoin)", *Forbes*, 15 May 2013, 24 July 2013 <<http://www.forbes.com/sites/kashmirhill/2013/05/15/the-feds-are-cracking-down-on-mt-gox-not-on-bitcoin/>>

⁵ Dominic Rushe, "US prosecutors: Liberty Reserve ran \$6bn money-laundering scheme", *The Guardian*, 28 May 2013, 24 July 2013 <<http://www.guardian.co.uk/business/2013/may/28/liberty-reserve-accused-money-laundering>>

⁶ "Exchange claims Thailand has outlawed bitcoin", *Finextra*, 30 July 2013, 30 July 2013 <<http://www.finextra.com/News/FullStory.aspx?newsitemid=25066>>

⁷ Jeremy Bonney, "Mt. Gox registers with FinCEN as a money services business", *CoinDesk*, 29 June 2013, 24 July 2013 <<http://www.coindesk.com/mt-gox-registers-with-fincen-as-a-money-services-business/>>

⁸ "Bitcoin Charts / Markets", *bitcoin charts*, n.d., 24 July 2013 <<http://bitcoincharts.com/markets/>>

⁹ "Virtual currency industry preps self-regulatory organisation", *Finextra*, 30 July 2013, 30 July 2013 <<http://www.finextra.com/News/FullStory.aspx?newsitemid=25069>>

Data intends to develop “technical standards and best practices intended to prevent money laundering and ensure compliance with applicable laws.”

A wildcard

In June, U.S. President Obama issued Executive Order 13645,¹⁰ which permits the United States to sanction foreign financial institutions who:

(i) knowingly conducted or facilitated any significant transaction related to the purchase or sale of Iranian rials or a derivative, swap, future, forward, or other similar contract whose value is based on the exchange rate of the Iranian rial; or (ii) maintained significant funds or accounts outside the territory of Iran denominated in the Iranian rial.

While this may seem to have no commonality with virtual currencies, this new sanction represents the first time that the United States is extending its oversight to currencies other than its own. Although it is, in some respect, an extension of previous sanctions placed on purchases by foreign governments of Iranian petroleum products, it opens up additional possibilities for new regulatory responses in relation to virtual currencies.

Next steps outside the United States

It is reasonable to expect that FinCEN's regulation of virtual currencies will be mirrored around the world. In the short run, there are two sets of jurisdictions that are likely to enact new regulations.

While it is part of the European Union, the United Kingdom is not part of the euro-zone. As such, it has more freedom to act independently to issue new regulations and more leverage to give them teeth. In a similar fashion, it is likely that FINTRAC in Canada, and AUSTRAC in Australia will issue similar restrictions in the name of restricting financial system access to Iranian and terrorist financiers.

It is also likely that the United States will look to influence leaders of Latin American countries that are major sources of and way stations for the narcotics trade to restrict the use of virtual currencies within their economies. Look for new regulation of Bitcoin and its brethren in Mexico, Colombia and, less likely, Bolivia.

Thailand's recent action brings up an interesting possibility: Will there be a rash of “Ban the Bitcoin” actions around the world? Certainly, it's low-hanging fruit. On the other hand, it's unlikely to deter criminals, who will just find another virtual currency to abuse, and will only truly inhibit legitimate low-value commerce — exactly the opposite of the desired effect. While such a ban would address some of the other potential deleterious effects of virtual economies, like the crowding-out effect that virtual currency commerce could have on the national currency-based economy, none of the current virtual currencies currently have the scale to effect national economies on a macro scale.

In the long run, transnational and international bodies are likely to address the risks of virtual currency-based money laundering and terrorist financing. Due to the longer time to implement such changes, it is conceivable that individual governments will implement new regulations, rather than waiting for an EU 5th Money Laundering Directive or new recommendations from the Financial Action Task Force (FATF) or the Wolfsberg Group.

Next steps for FinCEN and OFAC

The United States has a number of options for further ratcheting up the pressure on those who abuse virtual currencies. While Mt. Gox's registration with FinCEN may have lessened the impetus for further regulation, shifting of Bitcoin traffic to other exchangers, other national and international currencies instead of the U.S. dollar, or to other virtual currencies may require additional measures in the future. Which of those additional regulations is actually enacted depends on whether the focus of U.S. regulators is combating money laundering, or in further inhibiting the activities of already-sanctioned individuals who would be likely to use virtual currencies in their schemes.

The most limited enhancement to regulation would be for the Office of Foreign Assets Control (OFAC) sanctions on Iran, transnational criminal organization (TCOs) and/or narcotics traffickers to be extended to bar transactions in specified virtual currencies to those on the Specially Designated Nationals (SDN) List for those sanctions programs. The recent sanctioning of transactions denominated in the Iranian rial sets a precedent for such an action. By limiting the sanctions to

dealings with those who are already sanctioned, OFAC would not inhibit legitimate commerce in virtual currencies.

Another, more far-reaching step that could be taken is in FinCEN's court. It is within the limits of current regulation for financial organizations that deal in virtual currencies to be designated as institutions of primary money laundering concern (PMLC) under Section 311 of the USA PATRIOT ACT.

In similar fashion, financial organizations that transact in virtual currencies could be sanctioned by enacting new regulations that contain sanctions similar to those in the Iran Sanctions Act of 1996 (ISA), most notably the foreign exchange and banking transaction sanctions. Should these measures not prove onerous enough, those who dealt virtual currencies to those on OFAC's SDN List could find themselves on that list themselves, as facilitators of sanctioned activity or evasion of sanctions regulations.

Next steps for money launderers?

Do these potential turning of the regulatory screws mean that virtual currencies' days as money laundering vehicles are numbered? Perhaps not.

Consider that the goal of money laundering is to obscure — whether it is the source of funds or the beneficial owners of assets. Who is to say that there isn't a way to reasonably make a virtual currency look like something that isn't a currency?

Say, for example, that, instead of exchanging euros for Bitcoins, one bought shares in Bitcoin LLC, or “invested” in a Kickstarter-like venture. Once a person made their original purchase, the shares or investment could be “sold” to other shareholders at a mutually-agreeable price, regardless of their nominal value. Are the ownership stakes a virtual currency and thus subject to AML oversight, or are they not?

In that regard, Bitcoin and Liberty Reserve were victims of their transparency as virtual currency systems. One day, we may look back at 2013 as merely the first, easy round of a perpetual game of electronic Whack-a-Mole, where the little critters seem to get more numerous and seem to pop and disappear increasingly frequently. **▶**

Eric A. Sohn, CAMS, principal engagement manager, BankersAccuity, Skokie, IL, USA, eric.sohn@BankersAccuity.com

¹⁰Barack Obama, “Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Freedom and Counter-Proliferation Act of 2012 and Additional Sanctions With Respect To Iran”, *Federal Register*, 3 June 2013, 24 July 2013 <<http://www.treasury.gov/resource-center/sanctions/Programs/Documents/13645.pdf>>

FRAUD ANALYTICS:

Strategies and methods for detection and prevention

Looking for less theory and more hands-on methods for finding and flinging fraud from your business? Packed with countless software options and helpful tools, fraud analytics is the ultimate guide, with proven fraud detection and prevention strategies to get you started. Fraud analytics presents an effective approach to fraud detection that discovers unusual patterns, identifies masses of red flags, and aligns trends.

The following is an excerpt of the highly acclaimed Fraud Analytics: Strategies and Methods for Detection and Prevention.¹ A must-read for those in the private sector, academia and government.

Fraud analytics has become the emerging tool of the twenty-first century as it relates to detecting anomalies, red flags, and patterns within voluminous amounts of data that is sometimes quite challenging to analyze. The use of fraud analytic tools does not have to be complex to be effective. The techniques of criminals, and fraudsters, and their shenanigans are savvier due to technology and the means in which they use to hide fraudulent activities. While technology has played a role in increasing the opportunities to commit fraud, the good news is that it can also play a key role in developing new methods that can be used to detect and prevent fraud. In the past, a spreadsheet was the master of fraud analytics. However, a new revolution has taken us by force — new strategies, data mining techniques and powerful new software are constantly evolving.

Fraud analytics is used in auditing, detection and prevention. Fraud analytics depicts the elements of analysis that are used in today's fraud examinations and financial crimes investigations. It presents an effective approach to fraud detection that discovers unusual patterns, identifies masses of red

flags and aligns trends. What specifically is fraud analytics and how does it apply to the masses of fraud that often appear in media outlets, major newspapers and the like? *Fraud analytics is a way of life.* The fraud analytical theory exposes itself to the intricate details of discovery.

The actual analysis relies on the critical thinking skills of the fraud examiners or analyst's ability to integrate the output of these diverse methodologies into a cohesive actionable analysis product. The results of any fraud analysis or financial analysis should be easy to understand, clear and concise and easily transferrable to others involved in the case. Accurate identification is the most critical step in the fraud analysis process. It can positively impact detection, recommendations and resolutions. Fraud analytics imposes itself on the latest techniques where the application of varying tools can assist in detecting and preventing. (*ACL Analytics 10, CaseWare IDEA, Raytheon's Visual-Links Analytics, Actionable Intelligence*

Technology FIS, SAS Visual Analytics, Fiserv Fraud Risk Manager, Palantir, and Centrifuge Analytics)

A few of the techniques that fraud analytics is readily used for are the following:

- Link Association Analysis
- Financial Analysis
- Commodity Flow Analysis
- Net Worth Analysis
- Digital Analysis
- Threat Analysis
- Social Trend Analysis
- Event Flow Analysis
- Telephone Link Analysis
- Predictive Analysis (Modeling)

The objective of fraud analysis is to develop the most precise and valid inference possible from whatever information is available. The advantage of fraud analytics relies on anomalies. Within fraud analytics, anomalies are unintentional and will be found throughout the data set; fraud itself, however, is intentional.

Since the inception of fraud analytics, several methods have been used to assist in fraud detection and prevention. The first concerns accounting anomalies, internal control weaknesses, analytical anomalies, extravagant lifestyles, unusual behaviors, and complaints via ethics hotlines. With this perspective, keep in mind, that it is the examination and processing of information that results in the development of recognizable trends and patterns. *Fraud analytics is an entity of its own.* It covers a multitude of industries and can be used from the most complex and complicated to the simplest of fraud examinations, financial

Accurate identification
is the most critical
step in the fraud
analysis process

¹ <http://www.wiley.com/WileyCDA/WileyTitle/productCd-111823068X,descCd-description.html>

investigations and audits. No one technique is better than the other; they are all useful and much-needed tools.

A proactive approach to fraud analytics is the only way to stifle and to lessen the effect of fraudulent activities, which are at an all-time high in numbers and schemes. Aside from the security provided to customers, the amount of money saved by organizations is large considering the financial payoff of implementing a fraud analytics solution. Fraud analytics is not only used in law enforcement, the private sector has taken hold of its reigns and with all honesty they may have surpassed law enforcement in using the technique.

More law enforcement and private companies are finding and integrating fraud analytics within their everyday regime when working on investigations or merely conducting forensic accounting techniques. Fraud analytics is no different from any other source of analytics that has been used in the previous forms. A plethora of analysis strategies can be applied to detect the same anomalies; but fraud analytics has presented an innovative and forceful tool kit that is packaged in many formats.


Fraud analytics offers a sophisticated and savvy way to detect potential fraudulent activities before they occur. Data warehouses collect financial-based information and create what-if scenarios to identify how external factors and market changes affect sales, product mix and operations. These same technologies can be used to gather information and use the same type of predictive analytics techniques to identify suspicious patterns.

The tools available today enable us to analyze and collect information in a methodical, calculated manner. Fraud analytics has the capability to identify subsets of raw data, clean data, gather, and decipher all potentially relevant information. When one has to decipher the trends in the data and find patterns of usage and discrepancies to classify potential fraudulent activity, this capability becomes important.

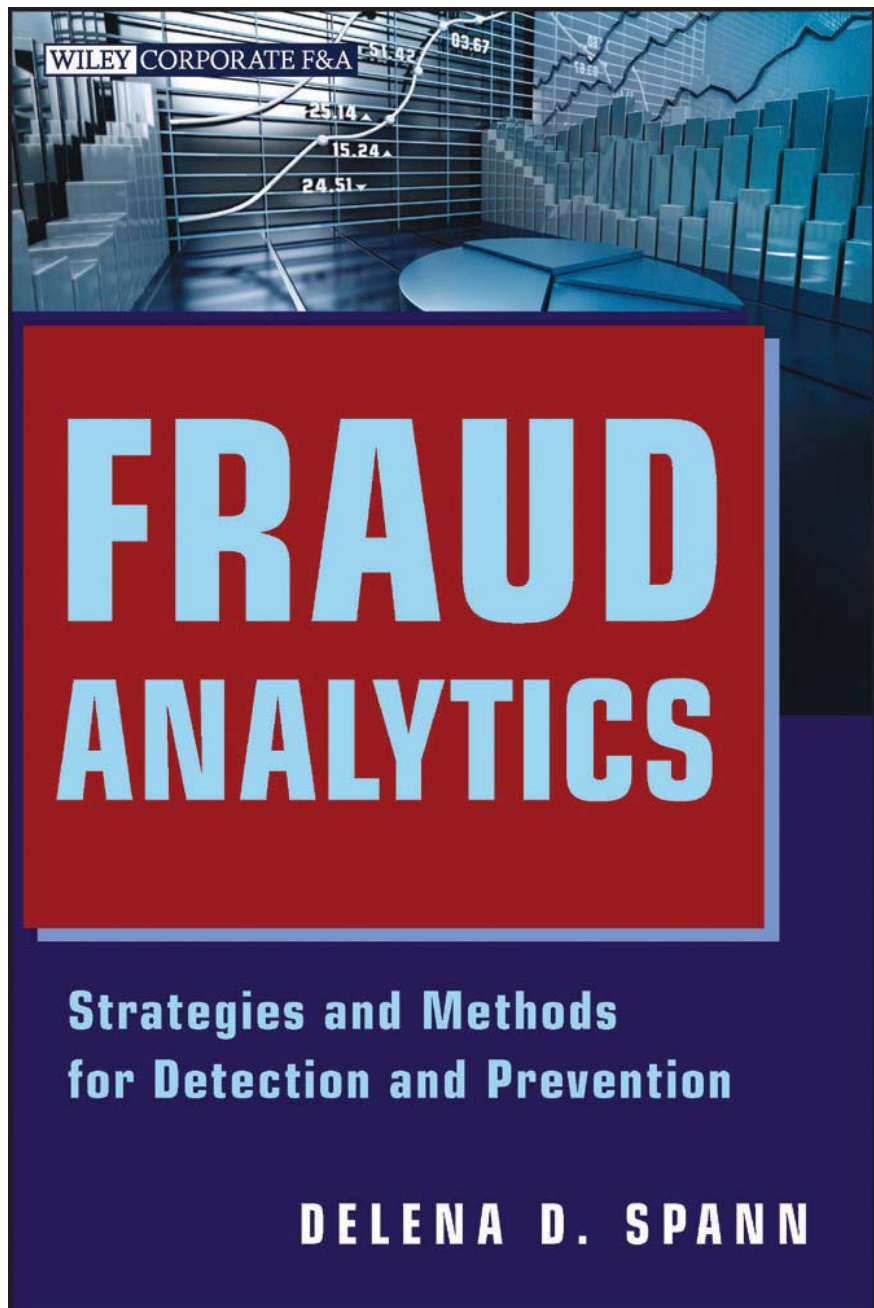
It has been said that the responsibility to combat fraud lies on the auspices of one's organization. Although fraud examiners and many other professionals can take the necessary precautions to protect themselves against fraud, we need to make a concerted effort to educate the masses on what they can and should do to protect themselves from such nefarious acts. The

cost of fraud can be astronomical in terms of financial loss and security breaches. With varied uses of fraud analytics, organizations can identify suspicious behavior and patterns before fraudulent activities occur.

Financial and intelligence analytics are designed to find patterns, associations and trends within data that people would not easily recognize. The same is true of fraud analytics, the recognition of patterns identifying potential fraudulent behavior represent the inception, not the end, of the analytical process.

The main difference between the use of fraud analytics and other applications of analytics is methodology. By implementing a solution to combat fraud, organizations are taking the first step toward a proactive approach. 

Delena D. Spann, MSc, CFE, CCA is employed by the United States Secret Service assigned to the Electronic & Financial Crimes Task Force where she serves as the financial analysis expert and conducts financial fraud analysis and examinations to detect the red flags, anomalies and patterns in financial crimes investigations.





REDEFINING DUE DILIGENCE:

A paradigm shift for AML/BSA compliance

Money laundering, terrorist financing and fraud pose an increasing threat to the integrity of the world's financial systems. The Bank Secrecy Act (BSA) of 1970, sometimes referred to as the anti-money laundering (AML) law, requires financial institutions in the United States to assist U.S. government agencies in the detection and prevention of money laundering by keeping records of cash purchases of negotiable instruments, filing reports on purchases of ten thousand dollars or more and reporting suspicious activity that might signify money laundering, tax evasion or other financial crime. Financial institutions must demonstrate that:

- they have implemented internal controls for BSA compliance
- there is independent testing to verify compliance
- there is a designated person(s) responsible for BSA compliance
- they provide adequate AML training for staff

Portions of the BSA were amended in 2001 under Title III of the USA PATRIOT Act to facilitate the prevention and detection of international money laundering and terrorist financing and the prosecution of perpetrators. Financial institutions active in the United States or transacting business in U.S. dollars are impacted by provisions of the USA PATRIOT Act that mandate adequate anti-money laundering and customer identification processes. The law requires financial institutions to develop a Customer Identification Program (CIP) appropriate to the size

and type of its business. The CIP must be incorporated into a bank's BSA/AML compliance program.

The global nature of financial and communication networks and the ease with which they can be used as a pipeline for illicit activities make worldwide collaboration an essential strategy for combating financial crime. Internationally, the Financial Action Task Force Recommendations, Wolfsberg Principles, EU Money Laundering Directives and the UNODC are indicative of the cooperative effort to create a broad network of AML regulatory provisions and policies.

New challenges face the global community following events such as the Arab Spring uprisings of 2011, the tightening of sanctions against Iran and the persistent evasion of current AML/CTF processes by drug cartels and corrupt political officials. Financial institutions must reinforce their fight against money laundering and terrorist financing by implementing tougher controls and expanding international cooperation while remaining compliant in a rapidly evolving regulatory environment.

The changing BSA/AML regulatory landscape

Regulators around the globe are responding to criticism of failed oversight of financial institutions with a newly energized focus on anti-money laundering and related risk. The recent spate of regulatory enforcement actions, significantly higher fines and massive media attention given high-profile cases like HSBC have bolstered institutions' AML efforts in 2013.

The Office of the Comptroller of the Currency's Semiannual Risk Perspective report issued in June 2013 stated that BSA/AML threats are increasing as a result of changing methods of money laundering and an increase in the volume and sophistication of electronic banking fraud, while compliance programs are failing to evolve or incorporate appropriate controls into new products and services.

Enforcement actions by the Department of Justice and the Securities and Exchange Commission (SEC) for insufficient due diligence on international business partners have pointed to several common problems:

- lack of timely and sufficient due diligence
- inadequate verification of information provided
- ignoring red flags that have been identified

Leveraging the media attention, both the Financial Crimes Enforcement Network (FinCEN) and the SEC announced plans to introduce new proposals for more proactive AML measures for broker-dealers and investment advisors. FINRA also indicated that its examination priorities would focus on AML, citing specific concerns with the level of due diligence on foreign bond currency conversion transactions.

Early this year, the European Commission announced the Fourth AML Directive intended to prevent money laundering and terrorist financing by strengthening AML rules in the EU. In addition, a new entrant into the AML arena, The Basel Committee on Banking Supervision, is proposing requirements for banks to include AML in

their enterprise-wide risk management. The committee also refers back to the Financial Action Task Force's global AML standards issued in 2012 and more recently issued guidelines. As further evidence of the worldwide focus on AML, the UK Financial Conduct Authority, Hong Kong Money Authority, New Zealand's Reserve Bank and Department of Internal Affairs and Financial Markets Authority have all ramped up their supervision by placing greater emphasis on AML risks.

The Federal Reserve Board recently demonstrated just how far the regulators are willing to go when they delayed the planned merger of a New York-based institution due to alleged shortcomings in their BSA/AML compliance program. Under a written agreement with the Federal Reserve Bank of New York, corrective action was mandated to include a revised firm-wide written BSA/AML compliance program, a revised written customer due diligence program, a written suspicious activity monitoring and reporting program and a six month suspicious activity look-back review.

Shortcomings in the current approach to KYC/CDD/EDD

Know Your Customer (KYC) and related due diligence activities are the foundation of a sound BSA/AML program. Financial institutions and other regulated companies are obliged to verify the identity of their customers at account opening, assess their customer risk, conduct ongoing due diligence of high-risk customers and monitor transactions to detect and report suspicious activity. Although the regulatory requirements are fairly clear, organizations are left to their own devices when it comes to the details of setting up effective AML programs and selecting the systems and tools to facilitate the labor-intensive processes for KYC, Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).

When sharing observations of industry issues at a recent ACAMS conference, representatives from the Office of the Superintendent of Financial Institutions (OSFI) presented their risk management expectations while contrasting what they actually see. EDD was of particular interest to these regulators after repeated examination findings showed EDD looking very much like standard due diligence. Their directive indicated that EDD

measures should be clearly distinguishable from baseline CDD. Based on their findings, they issued the following recommendations:

- Design EDD to ensure more attention is paid to higher risk customers and the attention is commensurate with the risk level
- Build an enterprise-wide risk assessment methodology and EDD approach across all business lines for consistent and appropriate identification and monitoring of high-risk clients
- Perform enhanced monitoring not only at point of sale/account opening but also at the transaction level
- Ensure that EDD measures apply to all high-risk situations and that they address and mitigate the risk factors identified
- Update customer information and changes to products, etc. in a timely fashion
- Implement effective CAMLO oversight.

Regulatory standards call for a risk-based approach that is appropriate to an institution's business. However, more often than not, risk is viewed as a static, point-in-time snapshot rather than a dynamic activity. Although regulatory guidelines address ongoing due diligence and adjustments to risk assessments based on changes in a customer's account profile and transactions, this is not the same as dynamic risk management. There is a disconnect with the real world of continual risk which begs the need for a dynamic risk model and the technology that can support it.

Due diligence redefined

To redefine due diligence, one must consider the dynamically changing global environment in which individuals and entities operate, the relevance of their social network or six degrees of separation and the nature and frequency of any related negative media.

The traditional buckets of high, medium or low risk customers present a one-dimensional view with no further differentiation on degrees of risk. A more accurate view and ranking of risk can be determined by analyzing an individual profile in conjunction with its social network (who they are linked to) and any negative media direct or through links. This methodology assigns a value to measure the degree of risk, making it much easier to identify and focus on the highest risk first. For example, in a risk-based approach using typical assessment criteria only (products, geography, historical


transaction amounts), a customer may be categorized as low risk when, in reality, once their links and newsworthiness are factored in they present a greater exposure to risk.

It becomes difficult, if not impossible, to stay ahead of the bad guys in an environment where sanctions, PEPs, news and other web information change constantly. Dynamic risk management calls for technical solutions that employ a daily surveillance model; however, finding the optimal balance of risk mitigation and alert management can be problematic. Introducing a classification or prioritization hierarchy into the screening technology orders alerts by risk and accuracy of the match. This provides a transparent framework from which thresholds can then be drawn based on an institution's requirements of what matches to review and in what order to review them.

Taking the first step forward

Globally, regulators and governments will continue to remain active in clamping down on AML failings. Institutions must now re-evaluate their programs and shore up any weaknesses. They can start the process by:

- Understanding the benefits of a shift from static to dynamic risk management
- Completing a cost/benefit analysis to assess the viability of keeping legacy systems and processes
- Exploring hosting alternatives to address budget and resource constraints
- Considering a principles-based versus rules-based methodology for entity resolution
- Implementing solutions that provide a more granular and interconnected view of risk with features for link analysis, link monitoring and news monitoring.

In a recent industry survey on the global cost of AML compliance, 66 percent of the 284 respondents in 46 countries saw an increase in their AML and OFAC compliance budgets over the last three years.¹ The option exists to continue spending money supporting traditional approaches with known gaps and shortcomings or to explore new methodologies that strengthen due diligence programs by identifying and prioritizing enterprise risk on a daily basis. 

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

¹ Veris Consulting, Inc. (2013). The global cost of anti-money laundering compliance [PDF file]: <http://www.verisconsulting.com>.

COURAGE IN COMPLIANCE

This is the true and compelling real-life story of a Bank Secrecy Act (BSA) and bank compliance officer. She had been recently hired by a small community bank. Shortly into her tenure at the bank, she realized something was seriously wrong. The compliance officer determined that the bank was processing an inordinate amount of transactions per month; well in excess of what a bank that size should have been handling. She learned that the bank was dealing with third-party processors and subsequently found out that the third-party processor's transactions were on behalf of Internet poker companies. The compliance officer knew this activity was illegal. She went to the bank president and other executives to attempt to exit the business relationships and file suspicious activity reports (SARs). Although the compliance officer continuously attempted to do the right thing, she was constantly rebuffed or misled.

What became apparent was that the tone at the top was not compliance friendly. Regardless of how dedicated and committed to doing the right thing a compliance professional is, if executive management does not adhere to a culture of compliance and exhibit the proper tone at the top, the compliance function is destined to fail. For approximately one year, the cultural conflict played out until state regulators closed the bank.

During that year, as the gripping story unfolded, the compliance officer experienced stress, sleeplessness, intimidation, guilt and fear for her safety. In addition, she incurred legal expenses to retain a lawyer. Despite her distress, she continued to try to do the right thing. As things progressed, the compliance officer cooperated with law enforcement and regulatory authorities.

Background

This saga contained various backstories involving a number of colorful characters. The law enforcement investigation began as an organized crime investigation into gambling. Organized crime led investigators to information regarding offshore payment processing in Costa Rica. Investigation led to third-party processing; processing for a range of illicit activities including gambling on Internet poker. Most banks would not wittingly service Internet poker companies. Third-party processors relied on shell and shelf companies, nominees, and other mechanisms to create the appearance that funds were being moved for legal and innocuous activities and not for illicit purposes.

What became apparent
was that the tone at
the top was not
compliance friendly

The focus of this case study is on third-party processors working with an insider at SunFirst Bank to process transactions for PokerStars and Full Tilt Poker. Developments in the multi-faceted investigation led the FBI to SunFirst Bank, a small community bank located in St. George, Utah.

The most important player in this aspect of the case is Cathy Scharf, the BSA and bank

compliance officer at SunFirst Bank. Her commitment to her compliance responsibilities is a demonstration of "courage in compliance."

Cathy Scharf is a Certified Anti-Money Laundering Specialist. She has over 25 years of experience in the financial services industry. Cathy joined SunFirst Bank as the BSA and bank compliance officer in 2010. She served in that position until 2011, when the bank was closed by state regulators. Cathy tried repeatedly to take action against illegal Internet account holders at the bank. She wanted to exit those relationships and file SARs. She was continuously rebuffed by bank officials, including John Campos, vice chairman of the board of directors and part owner. This experience took a personal and emotional toll on Cathy.

Law enforcement conducted a long term investigation, which was initiated based on wiretaps conducted by the Rockland County, New York Sheriff's office. The case was referred to the Federal Bureau of Investigation (FBI) based on organized crime implications. The FBI was assisted by Homeland Security Investigations (HSI) and the New York High Intensity Financial Crimes Area (HIFCA) task force. The investigation started as an organized crime case that evolved into an investigation of money going into illegal Internet gambling. The government dedicated considerable time and resources to this investigation. The investigation involved three waves of indictments, the first focused on organized crime; the second on payment processors; and the third on poker companies. SunFirst Bank was one of about 12 banks involved in the payment process.



Law enforcement sources described SunFirst Bank's processing activity as blatantly unreasonable considering its size. The poker companies, through third-party processors, were able to exploit the fact that SunFirst Bank was undercapitalized and required an infusion of funds. Law enforcement sources advised that this was a multi-dimensional long term investigation that led to many subjects. Over the course of time, they required considerable information from U.S. banks. Law enforcement sources noted that they received outstanding cooperation from the U.S. banks with which they dealt.

Scheme to defraud

The scheme evolved based on the fact that banks were largely unwilling to process payments for illegal activity such as Internet gambling. PokerStars, Full Tilt Poker and Absolute Poker used fraudulent methods to avoid restrictions and receive billions of dollars from U.S. residents. Money received from U.S. gamblers was disguised as payments to hundreds of non-existent online merchants and other non-gambling businesses. The poker companies relied on highly compensated third-party processors through the creation of phony companies

and web sites used to disguise payments to the poker companies. Poker companies and third-party processors conspired together to deceive banks.

Knowing that banks were not permitted to process payments related to Internet gambling, third-party processors established mechanisms to circumvent the law. They operated through deceptive means designed to trick U.S. banks into processing gambling transactions on behalf of Internet poker companies. Some of the mechanisms they used included:

- Fraudulent credit card processing, wherein the processors falsified transaction codes
- Use of prepaid credit cards that were loaded with funds from credit cards
- Fraudulent e-check processing wherein transactions appeared to be non-gambling transactions through the creation of phony companies and web sites

When the poker companies lost substantial money because e-check processing was frozen by and forfeited to law enforcement, the poker companies wanted processors to

find "transparent" processing. This meant that the poker companies wanted the processors to find banks who knew they were processing online gambling proceeds and who were willing to facilitate this activity, although it was illegal. Processors found a few banks like SunFirst Bank who were facing serious financial difficulties and as a result agreed to accept the online gambling transactions. They referred to this as "transparent" processing.

The link between the online poker companies and SunFirst Bank began with Chad Elie. Chad was a third-party processor who processed transactions for PokerStars, Full Tilt Poker and Absolute Poker. He needed a bank he could work with as a transparent processor. Enter Jeremy Johnson. Jeremy was an alleged telemarketing fraudster who is still under investigation by the Federal Trade Commission (FTC). He met Chad Elie at an online marketing symposium in Las Vegas. Chad and Jeremy formed a processing company together, Elite Debit. Jeremy had a bank, SunFirst Bank. Employees of the bank used to joke that SunFirst Bank was "the bank of Jeremy Johnson." SunFirst Bank was experiencing financial difficulties and

they enlisted Johnson to be an investor and part owner. Jeremy introduced Chad Elie to John Campos, vice chairman and part owner of SunFirst Bank. Elie promised to invest \$10 million in the bank and to bring in millions of dollars through processing transactions for the online poker companies. Campos agreed with “trepidations” about the gambling processing.

SunFirst Bank was a beneficiary of the real estate boom in 2006 and subsequently a victim of the subprime mortgage crisis in 2008. The bank found itself seriously undercapitalized. In October 2009, the Federal Deposit Insurance Corporation (FDIC) ordered SunFirst Bank to increase its capital reserves by at least 11 percent. In December 2009, following investments in the bank made by Johnson and Elie, the bank began processing Internet poker transactions. SunFirst Bank processed more than \$200 million in payments from PokerStars and Full Tilt Poker from December 2009 to November 2010. Elie and Johnson paid John Campos what Campos described as a “bonus” of \$20,000. The indictment handed down in this case described the payment to Campos as a “bribe.” State regulators shut down SunFirst Bank on November 4, 2011.

April 15, 2011, was referred to as the poker world’s “Black Friday.” On that date, the U.S. Government seized the domains of the three largest online poker sites servicing the U.S. market, PokerStars, Full Tilt Poker and Absolute Poker. A number of indictments

were handed down to founding members and executives responsible for the three online poker companies. John Campos and Chad Elie were also indicted and were subsequently convicted for their roles in using SunFirst bank to facilitate the processing of illegal gambling activity. Jeremy Johnson was not charged in this case. However, he was indicted as a result of the ongoing FTC case, involving his company I Works, in what has been described by the FTC as one of the largest and most intricate online marketing frauds ever perpetrated in the United States.

Lessons learned

From the time she was hired as the BSA and bank compliance officer, in the summer of 2010 until SunFirst bank was shut down in November 2011, Cathy Scharf dealt with the illegal processing of online poker transactions as the bank’s compliance officer. By her own account, she was in the wrong place at the right time. Cathy repeatedly told the bank president and other executives that they had to exit customer relationships and file SARs. The president and other executives regularly made misrepresentations about addressing compliance issues. They continued to conduct business as usual. This clearly demonstrated that the tone at the top was poor and not compliance oriented. To Cathy’s credit, she remained undeterred and tried to perform her compliance duties and do the right thing. As the case unfolded, Cathy cooperated with authorities, despite

attempts made to intimidate her by lawyers representing the bank. This case study demonstrates the importance of the BSA compliance officer and the compliance function. Compliance professionals are truly on the front line in the fight against fraud and money laundering. One of the strongest lessons learned was that if the tone at the top in an organization does not support a culture of compliance, the compliance function is in serious trouble. Doing the right thing can be challenging under good circumstances. Doing the right thing under bad circumstances can be a nightmare, as Cathy experienced. In the end, no matter how difficult, doing the right thing is always the proper course of action to take.

When asked if confronted with a similar situation would she do the same thing again, Cathy responded unhesitatingly that she would, however she would do it differently. Among other things, Cathy would have spoken to authorities sooner; she would have convinced another bank employee, who also did the right thing, to go speak to authorities when she did; and she would have taken a different course of action regarding SARs.

For standing up to a constant and stressful challenge regarding her compliance responsibilities at SunFirst Bank, Cathy Scharf demonstrated “courage in compliance.” **A**

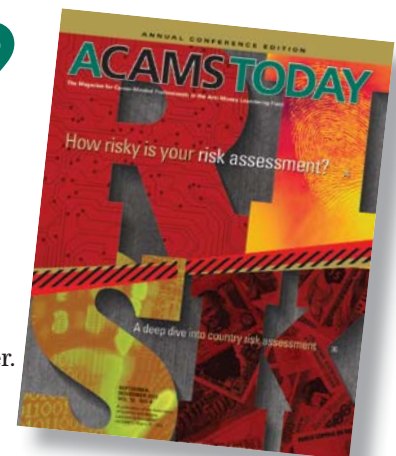
Dennis Lormel, CAMS, president and CEO, DML Associates, LLC, Lansdowne, VA, USA, dlormel@dmlassociatesllc.com

Reading someone else’s copy of

ACAMS[®] TODAY?

Join ACAMS and you’ll receive your own copy every quarter, plus:

- Unparalleled networking with leading professionals in the field.
- Significant discounts on education and training through conferences, seminars, workshops and webinars.
- Professional advancement via ACAMS’ worldwide Career Development Center.
- Accreditation as a Certified Anti-Money Laundering Specialist (CAMS), the most globally-respected professional credential in the industry.



ACAMS[®] | Advancing Financial Crime Professionals Worldwide

For more information and to join contact us by:

Phone +1 (866) 459-CAMS Outside U.S.: +1 (305) 373-0020 Fax: +1 (305) 373-7788 or +1 (305) 373-5229
Email: info@acams.org Online: acams.org ACAMSToday.org acams.org/espanol



Protect your organization from a world full of risk.

Rely on compliance, due diligence and verification
solutions from LexisNexis®.

Don't blink

Risk is clever, unrelenting and it's stealthy. One false move can create a gap in your defense resulting in a tarnished reputation, heavy fines, and a compromised bottom line.

LexisNexis® understands the nature of risk and delivers AML/compliance, risk mitigation and enhanced due diligence solutions to help you proactively manage it. Solutions such as LexisNexis® Bridger Insight™ XG which now offers unparalleled protection with 100% global sanctions coverage and access to BankersAccuity's Global WatchList® data.

See for yourself how LexisNexis can help you protect your organization from a world full of risk with a **30-day free trial*** of Bridger Insight XG.

Contact us today at 888.286.3282
or visit lexisnexis.com/risk/freetrial

*Complete offer details at lexisnexis.com/risk/freetrial

XCELENT Service 2013

LexisNexis Bridger Insight XG
is the winner of Celent's
2013 XCelent Service Award
for global watchlists and
sanctions.



Risk Solutions
Financial Services

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Bridger Insight is a trademark of LexisNexis Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2013 LexisNexis. All rights reserved.

How risky is your risk assessment?

would like to begin by asking readers to conduct a brief visualization exercise. Read the following and then close your eyes and think of the first thing that comes to mind.

Risk Assessment.

For most, I am guessing the two simple words conjured images of risk formulas, controls, or the intoxicatingly popular heat map. After all, inherent risk less the effectiveness of mitigating controls equals residual risk. Written another way $IR - CE = RR$. Regardless of your preference, a simple formula does not a risk assessment make. For those who read risk assessment and imagine new product development, dynamic customer risk models, calibration of transaction monitoring scenarios or role based employee training — congratulations on your advanced risk assessment vision! If you would like to refine your vision even more, read on.

This article will go beyond traditional risk assessment mechanics in favor of practical, actionable and easily implemented best practices. After all, the true test of the efficacy of your risk assessments is not the birth of a green three on an XY axis or a menacing red sphere in the dreaded upper right quadrant of a heat map. Rather, efficacy will be determined by your methodology's ability to withstand microscopic scrutiny; to serve as the foundation for a risk-based program that adapts to internal and external changes; to provide a reliable means for the institution to make effective decisions regarding human resources, capital and other allocations; and to provide assurance to key stakeholders regarding your organization's risk management practices.

It would be fatuitous to write an article on risk assessments without acknowledging the guidance provided by the Federal Financial Institutions Bank Secrecy Act/Anti-Money Laundering Examination Manual (exam manual). The exam manual describes a two-step process including the development of risk categories (i.e., products, services, customers, entities, transactions and geographic locations) and the requirement to conduct a more detailed analysis of the data to better assess the risk within these categories.¹ The exam manual also eloquently articulates its neutral position on the appropriate

method and format, which leaves AML officers and risk practitioners to make sense of the remaining 417 pages.

This article is divided into two parts. Part one focuses on the execution of the risk assessment, while the second part provides examples of actions you can take to effectively leverage the risk assessment results across the enterprise.

The first objective of the risk assessment is to identify the appropriate scope. Fortunately, the exam manual provides extensive guidance on specific risk factors within each risk category. These include the always popular acronyms such as PEP, NRA, CIB, HIFCA, NBF and RDC. However, how many risk factors does your risk universe include that are not set forth in the exam manual?

Regrettably, when presented with a seemingly straight forward two-step process and library of risks it is all too easy to lose sight of a risk assessment's true objective. After all, the risk assessment establishes your organization's risk profile and provides a mechanism for the development of appropriate risk management strategies. While knowing whether you have 6 or 14 PEPs under your roof is useful, there are "hidden" risk factors that also deserve your attention in combating money laundering. Therefore, a holistic risk universe should also consider control risk factors. Identified independently or through collaboration with a broader enterprise-wide risk function, control risk factors — not to be confused with controls themselves — are often at the root of AML program failures.

Employee risk is one such risk factor and is at the heart of several recent high profile enforcement actions. For example, are controls in place to ensure a rogue account officer cannot override risk scores of the customer risk model you have worked so hard to develop and hopefully calibrate on an ongoing basis.

Perhaps the most heavily debated risk assessment topic is the anatomy of the risk scoring engine. Inherent risk is generally defined as the "pure" risk that a particular requirement poses to an entity in the absence of any actions management might take to alter its likelihood and/or impact. Should a qualitative risk score give way to a quantitative approach, and if so, what is the most appropriate numeric range; 1 through 5, or is 1 through 50 more appropriate? Perhaps

inherent risk is best attacked through a multi-dimensional risk score that takes into consideration impact and likelihood? Regardless of the approach selected, the critical success factor in developing the risk engine lies in establishing clearly defined and documented explanation of each risk level. For example, a range of 1 to 50 could be ideal so long as the difference between a risk score of 27 and 28 is clearly delineated. This delineation should also go beyond the severity of adjectives in risk statements, for example highly likely vs. somewhat likely and include quantifiable data. This brings us to our next pain point — data, data, data!

The role data plays in the risk assessment process cannot be overstated. Data provides the foundation upon which to base risk decisions. Implementing a robust data support

Data provides the
foundation upon which
to base risk decisions

role includes developing an inventory of where data resides across the organization, understanding how data is collected, stored and updated and conducting periodic testing to ensure its accuracy. Once this process is complete, a comprehensive key risk indicator (KRI) library should be developed. Your organization's risk profile is subject to change every day you are in business and KRIs provide key stakeholders with a measure to monitor ongoing risk and identify potential vulnerabilities in their control environment. An example of AML KRIs include, but is certainly not limited to, the number of high-risk customers, type and volume of transactions, investigation escalation percentages, SAR volumes and employee turnover.

No risk assessment article would be complete without a discussion on controls. Controls and their associated control score, act as the fulcrum between inherent and

¹ The FFIEC's 2010 Bank Secrecy Act/ Anti-Money Laundering Examination Manual Risk Assessment — Overview page 22

residual risk. Traditionally, risk assessments involve making a control design effectiveness decision that does not include a more detailed operating test effectiveness. Nevertheless, understanding your control environment should involve the use of multiple data points to ensure the most accurate design effectiveness assessment possible. Control data point should include control type automated versus manual and control focus preventative vs. detective. These classifications, while useful, are not sufficient when used in isolation, and should thus be leveraged holistically. For example, the robust preventative and automated transaction platform is certainly a must but what if installation occurred last week? This introduces the concept control maturity. Control use and control review are among a dozen or more additional factors that can assist with making a more educated control design effectiveness decision and serve as the roadmap upon which to develop a control testing plan.

Last, but certainly not least, we arrive at residual risk. Residual risk is the remaining risk after management has taken action to alter inherent risk through the implementation of controls. However, identifying residual risk must be viewed as the end of the beginning rather than the beginning of the end, as much work is left to be done once the heat map is in hand. Regardless of whether a residual risk score is automatically derived based on control design effectiveness or manually calculated through a thorough management review practice, the residual risk profile should become the play-book for integrating risk assessment results into the organization's business practices.

Before we dive into part two it is important to note that in the time it has taken you to arrive at this paragraph your organization's AML risk profile has changed. Customers have been onboarded, correspondent banks have processed transactions, cash has changed hands and changes to staffing may have occurred. Organizations are well advised to proactively assess their risk through the use of the aforementioned KRIs as well as a robust interim risk assessment process.

An interim risk assessment process should touch major lines of business and include an evaluation of potential red flags such as violations or non-compliance with regulations and policies, department or business

line metrics including vacancies and turnover, and changes to product offerings, risk models, third party relationships and department systems. This process is easily implemented through a formal checklist. The result of this evaluation provides management with a tool for identifying the need for more robust interim assessments and demonstrates a robust and proactive risk management culture.

So you have diligently defined your scope, developed your scoring engine, evaluated your controls, derived residual risk and even taken the time to develop a snazzy gradient shaded matrix depicting your organization's risk in vibrant red, green and yellow. Congratulations...now what?

At a minimum an organization's risk assessment can effectuate change to a dozen or more elements of a comprehensive AML program

Recent surveys suggest that organizations struggle to derive value from their risk assessment. When you consider the fact that a risk assessment has the potential to shape almost every aspect of an organization's AML program, it is disheartening to see the exercise conducted and the results left in the ether to await an annual update. At a minimum an organization's risk assessment can effectuate change to a dozen or more elements of a comprehensive AML program. Three such opportunities are described below.

Enhanced Due Diligence: As we have learned, "customers" are a primary risk assessment category. Let us pretend that through the risk assessment process your organization has determined that MSBs represent the highest risk customer type

based on the extensive use of supporting data of course. Why then does the enhanced due diligence (EDD) process use a one size fits all approach? Ideally, a MSB specific EDD form would be developed to address the additional risk presented by this customer type.

Transaction Monitoring Scenario Coverage: With customized EDD addressed, let us say that your risk assessment has also determined that correspondent banking reflects a high risk activity. Does your transaction monitoring system have a rule or scenario to monitor this high risk activity? Organizations should perform an annual assessment to map the results of the risk assessment to production scenarios to ensure appropriate coverage exists for those transaction types presenting increased risk.

Targeted Training: Recent enforcement actions have highlighted the failure of a one size fits all training approach. One of the easiest opportunities to embed risk assessment results is in an organization's training curriculum. Rather than look for providers with the latest tablet training capabilities, focus on your organization's highest inherent risk categories and develop modules specific to these risks. For example, if the NRA population presents elevated risk to your organization, ensure training for employees who work with this population have received additional education focusing on the unique risks presented by this customer type.

In summary, I suspect few will question the importance of the risk assessment process. However, I would encourage readers to question the risk their risk assessment creates. As money laundering schemes grow, increasingly complex organizations must develop and evolve their process to go beyond the mechanics of updating three dozen risk factors and instead fully embrace a risk identification and mitigation strategy to commensurate with the level of sophistication of those who are intent on exploiting it. To close, please indulge me in one last visualization exercise. When you read the following words, what comes to mind? Ready?

Risk Assessment. 

Michael Florence, CAMS, anti-money laundering practice leader, Treliant Risk Advisors, Washington, DC, USA, mfflorence@treliant.com

19TH ANNUAL INTERNATIONAL AML & FINANCIAL CRIME CONFERENCE

**SAVE
\$400***
by Oct. 25 with code PT-400

March 16-19, 2014 • The Westin Diplomat • Hollywood, Florida



KEYNOTE SPEAKER

Juan C. Zarate

Senior Adviser, **Center for Strategic and International Studies**

Senior National Security Analyst, **CBS News**

Visiting Lecturer of Law, **Harvard Law School**

Former Deputy National Security Advisor for Combating Terrorism

Former Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes



The AML community's
most trusted and
relevant international
programming

SHARPEN



Financial crime
prevention thought
leaders and the most
influential government
officials

CONNECT



The world's preeminent
forum for executive
networking and global
intelligence

DEVELOP

Register Today! • moneylaunderingconference.com • +1 305.373.0020 • info@acams.org

*Register and pay using VIP code PT-400 by October 25, 2013, and save \$400 off the standard, non-government main conference price. Virtual conference option does not qualify for this discount. Pre-conference workshops and the CAMS Examination Preparation Seminar are not included in main conference pricing. Please contact Geoffrey Fone at gfone@acams.org or at +1 786.871.3021 for group discount rates. Discounts cannot be combined.



PARTNER SHARE SYNERGY COOPERATE COLLABORATE

Partners in anti-crime —Law enforcement outreach enhances BSA/AML programs

In the Bank Secrecy Act (BSA) compliance community there is often a lot of discussion about creating better partnerships with law enforcement. While some organizations make this a priority, others do not always realize the value of an outreach effort. The fact is that an outreach program can greatly enhance a compliance program and pay dividends in supporting everyone's primary objective of stopping money laundering and related crimes.

From a purely compliance perspective, the various regulatory agencies are primary "customers" for financial institutions and Money Services Businesses (MSB). However,

from a business perspective, the compliance department's primary customer is law enforcement. That is because the requirement to file Suspicious Activity Reports (SARs) produces the top "product" that this highly specialized consumer group wants and needs.

Law enforcement agencies comb the Financial Crimes Enforcement Network (FinCEN) database for case leads. If the quality, quantity and availability of this data are high, then it becomes a more valuable commodity, especially as the capabilities of law enforcement data and text mining tools have become more technologically advanced and sophisticated.

These data mining capabilities make your SARs a much more effective tool for identifying terrorist financing, money laundering, fraud, embezzlement, income tax evasion, as well as other crimes.

So as law enforcement is your principal customer, who better to partner with and to establish a strong and long term relationship than law enforcement? The benefits are two-fold: First law enforcement representatives can learn more about your data and how it is collected. This might enable them to create more specific and therefore, easier to manage information requests. The end result is greater efficiency on both ends. Second,

financial institutions and MSBs can become more aware of the kind of data that is most useful to law enforcement and can therefore focus on ensuring that such data becomes a focal point for a compliance program.

Yet making this data the most useful requires cooperation, partnership and mutual trust. Law enforcement can't expect compliance officers to inherently know what they are looking for and compliance professionals, while well-trained and talented, are very rarely expert mind readers. Also even the best compliance programs can always be enhanced, updated and strengthened. Ensuring that this ongoing process provides law enforcement with better data makes the joint AML effort that much better.

It is important to note that while outreach programs can be a very valuable part of any financial institutions' BSA/AML program, the institutions should always abide by the BSA/AML regulations as well as their internal policies and procedures. Do not become complacent, by providing documents to law enforcement that they are not entitled to receive without a subpoena! These programs are beneficial to both law enforcement and the financial institutions, but violating either BSA/AML regulations, law enforcement procedures or the financial institution's policies and procedures could cause irreparable harm to the program. That is why communication is often the key to success and legal responsibility.

With that in mind it becomes obvious that establishing communication is the first step in any outreach program. One of the easiest ways to begin such an effort is to contact your local SAR review team or other similar law enforcement equivalent. SAR review teams have been established in most U.S. Judicial Districts. The advantage of establishing a relationship with a SAR review team is that normally representatives from most, if not all, of the federal law enforcement agencies and in many cases state and local law enforcement agencies are represented on those teams.

Therefore, establishing a relationship with your local SAR review team will give you access to multiple law enforcement agencies. In many cases you may identify a SAR that in your opinion should be reported directly to law enforcement; however, you may not be certain which law enforcement agency should be contacted. Reporting the SAR to a SAR review team makes this decision easier for you. Once reported to the

SAR review team, the SAR will be discussed with the members of the team and assigned to the appropriate law enforcement agency. However, you should also maintain contacts with specific federal, state and local law enforcement agencies. When you identify a SAR that you believe a specific agency would investigate, you have the option of contacting that law enforcement agency directly.

Once you have established the line of communication, the process of creating an environment of partnership and trust with your law enforcement contacts can begin. How this is done will be unique to your organization and the law enforcement groups with which you work. So while there is no "right way" of going about this, the following examples might provide a framework that meets the needs of your organization.

Financial institutions may supplement their BSA/AML training programs — one of the four pillars of an AML program — by inviting law enforcement agents to assist with BSA/AML training. The advantage of law enforcement training presentations includes, but is not limited to the following:

- Inviting law enforcement helps to establish and build the trust and partnership between the agency and your financial institution.
- Law enforcement will often provide guidance related to new money laundering trends, methods and techniques; which provides the financial institution with the ability to tune their AML transaction monitoring tools, as well as recognizing customer activity that previously may not have appeared to be suspicious. Understanding money laundering techniques; in addition to customer due diligence and other factors is one of the keys to recognizing suspicious activity.
- Law enforcement will often use case studies to demonstrate various money laundering methods and techniques. In many cases financial institution employees will recognize suspicious customer activity and/or transactions that they previously considered explainable; the case studies have proven to be one of the best BSA/AML training tools. This is another opportunity for the institution to tune their AML transaction monitoring tool.
- Law enforcement familiarizes the financial institution with the most appropriate agency to contact when the financial institution detects what they suspect to be

money laundering or one of the underlying crimes that leads to money laundering that should be immediately brought to the attention of law enforcement.

- Law enforcement agencies will often provide guidance related to new cases that involve penalties or even prosecutions against financial institutions. Lessons learned from these cases also provide guidance for program enhancements to the financial institution.
- Law enforcement agencies will also discuss new regulations and regulatory guidance, both of which are extremely helpful with enhancements to the financial institutions BSA/AML program.

Establishing communication is the first step in any outreach program

Once partnership and trust have been established, law enforcement, including SAR review teams, may invite financial institutions to their regular meetings. Participation in these meetings will provide added insight into new money laundering trends and techniques and provide financial institutions with an appreciation of how law enforcement uses the SARs filed by financial institutions to develop cases, including money laundering, terrorist financing as well as other underlying crimes, the proceeds of which are subsequently laundered.

Law enforcement can not disclose the contents of SARs to financial institutions; however, suspect and other identifying information may be redacted in order to provide examples to improve BSA/AML transaction monitoring tools, the investigation of alerts generated by those monitoring tools, customer due diligence, SAR decisions and SAR quality. For example during the customer due diligence or enhanced

due diligence process, discussion with law enforcement will often provide suggestions or ideas related to customer interviewing techniques that will be useful during discussions with customers who appear to be conducting suspicious transactions. Those suggestions may include, but are not limited to, documenting: How the customer reacted to questions asked by the financial institution; customer comments in response to the financial institution's inquiries; for cases that involve currency, how the customer carried the currency, how it was bundled or packaged, if it had a particular smell; and if possible to retain surveillance photographs or video. A surveillance photo of the target of an investigation with a large stack of currency in front of them at the teller window fits the old cliché; and in this case it is worth at least a thousand words!

Financial institutions often detect customer activity and or transactions that they can not identify as suspicious activity, but they are not comfortable clearing as not suspicious. While law enforcement normally will not instruct them to either file or not file a SAR, the financial institution will have the opportunity to discuss the customer activity with their law enforcement counterparts. During the discussion the financial institution may provide law enforcement with information related to the customer's business or anticipated activity and the deviation from the anticipated activity. Based on that information law enforcement may be in a position to provide their knowledge of the customer's business based on previously prosecuted cases. This information could help the financial institution to be in a better position to determine if the customer's activity is suspicious or explainable.

In cases where the financial institution determines the activity or transactions are suspicious, the information provided by law enforcement may also provide the information that will assist the financial institution with preparing a better SAR narrative. The narrative enhancements may include covering the five "W's" (who, what, when, where and why) and how; key words that will add value to the SAR narrative, identifying the victims of the crime if any, all known contact information and others involved in the suspicious activity. Law enforcement may also provide ideas about how to summarize the suspicious activity, which will provide a more valuable SAR to law enforcement and save the filing institution valuable time with the SAR preparation.

Financial institutions often make the decision to close an account relationship due to suspicious activity in that relationship. However, law enforcement, in response to filed SARs, may request that the financial institution maintain the account relationship because while closing the account relationship is not considered "tipping off" the customer that a SAR has been filed; the customer may assume that their suspicious activity has been detected and they may

Establishing a relationship with your local SAR review team will give you access to multiple law enforcement agencies

therefore cease conducting the activity or move to another financial institution. Either of these courses of action will hinder law enforcements' investigation and in some cases may cause irreparable harm to the investigation including discontinuing the investigation.

On the other hand, law enforcement requests to keep an account open when the identified suspicious activity is a fraud that over time would cause the financial institution to lose money should not be honored. Normally explaining that the financial institution would lose money because they are the victim of the fraud will be understood by law enforcement; especially when the financial institution has an effective law enforcement outreach program.

An obvious concern that needs to be addressed is that establishing such a close relationship with law enforcement could reveal issues with a compliance program that requires correction or updating. There are two ways of looking at this. The first is making it a practice of keeping law enforcement at arm's length. That might produce the situation that if they come across information that would open an investigation, there could be a sense that there is more going on than meets the eye. That is simply because they are not familiar with your program. On

the other hand, establishing a law enforcement outreach program allows financial institutions to demonstrate to law enforcement that they have implemented an effective BSA/AML program including leading industry practices; however, no program is perfect. Financial institutions can not and are not expected to detect every suspicious transaction and/or suspicious activity that occurs. Therefore in cases where the financial institution does not detect and report suspicious activity related to a customer or a particular type of activity, law enforcement will not be quick to initiate an investigation of the institution.

Let us explore a hypothetical case. A money launderer agrees to cooperate with law enforcement and states that he has laundered funds through your financial institution. While he may have conducted transactions at your institution, he may be exaggerating the volume of activity. As a result of the informant's statement law enforcement may initiate an investigation. Once the financial institution is alerted to the investigation, it will likely engage outside counsel to represent the institution; which in addition to the fees causes a disruption of business. However, a law enforcement outreach program may prevent the investigation.

Make no mistake, outreach programs are not a "Get Out of Jail Free" card. However, when your institution works with law enforcement and they know first hand that you have an effective BSA/AML program, it greatly reduces the likelihood in many cases that investigations would be initiated.

Creating and maintaining an outreach program with law enforcement is a significant initiative and should merit all the business case research and review that any major effort deserves. It requires sound management and communication skills and resources. Like any good long-term relationship, it should not be entered into lightly. However, most compliance programs will discover that such a relationship builds a partnership that benefits all concerned and will produce results now and in the future. **TA**

Don Temple, principal, BSA/AML consultants LLC, Fallston, MD, USA, donalddt1@yahoo.com

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



**Delivering Compliance
Program Strategic Vision.**

**Driving Program
Transformation Support.**

**Enabling Risk and
Compliance Analytics.**

The financial industry today is dealing with the ever-increasing challenges of combating financial crimes to include money laundering and terrorist financing. Booz Allen Hamilton offers comprehensive regulatory compliance and risk management solutions to assist organizations with mitigating problems and developing cost-effective and efficient operational strategies. Our services leverage experience in supporting regulatory agencies as well as commercial financial institutions by providing subject matter expertise in a variety of areas including Anti-Money Laundering (AML), Office of Foreign Assets Control (OFAC), and Anti-Bribery and Corruption (ABC) regulations.

For more information on how Booz Allen can help your organization manage your regulatory compliance strategies, contact Daniel Tannebaum at Tannebaum_Daniel@bah.com. See our ideas in action at boozallen.com

Booz | Allen | Hamilton

delivering results that endure

NEGATIVE NEWS

— Discovering and verifying entity due diligence information

Compiling negative news information about entities is a dynamic process. Assembling static entity information like name, date of birth and tax numbers is only the first step in entity identity and information management. Present day KYC/CIP/EDD requirements for onboarding, customer risk rating, beneficial ownership, FCPA compliance, look-back investigations and sanctions reviews are just a few of the drivers that have financial crimes professionals utilizing negative news for their practices.

Unlike information derived from credit sources or verified financial documents, negative news data may have content that is not risk relevant or can't be verified. Historically, negative news obtained from using wide-spectrum search methodology has resulted in horrendously high levels of noise, false positives, unrelated material, and content that is numerous generations removed from the original data or information source. In addition, information that has been sunsetted or removed from public access, will not be derived from wide-spectrum negative news research that does not include cataloged data from diverse and disparate information sources. One of the greatest challenges is to get risk relevant

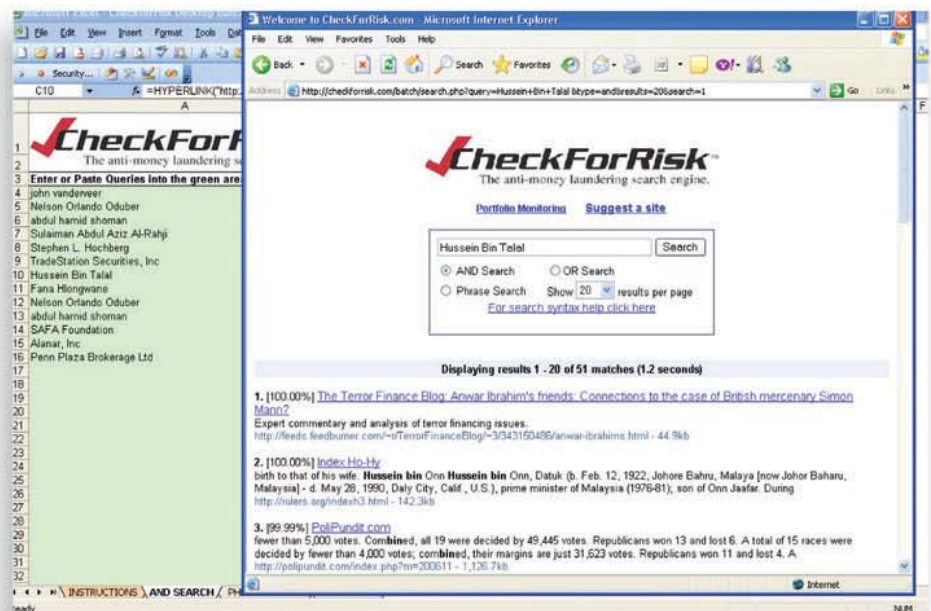


Figure 1

information into the work bucket of the analyst. Irrelevant information that is developed or alerted creates additional work that must be cleared from entity investigations.

Search methodology that mitigates the noise should include indexing only risk-relevant information so analysts are not deluged by

unrelated search results. The need to continually update and document entity searches is also of great importance. Hyper-targeted data mining with the core data collection re-indexed and updated every 24 hours with an audit trail should be systematic to the research process. Special attention should be

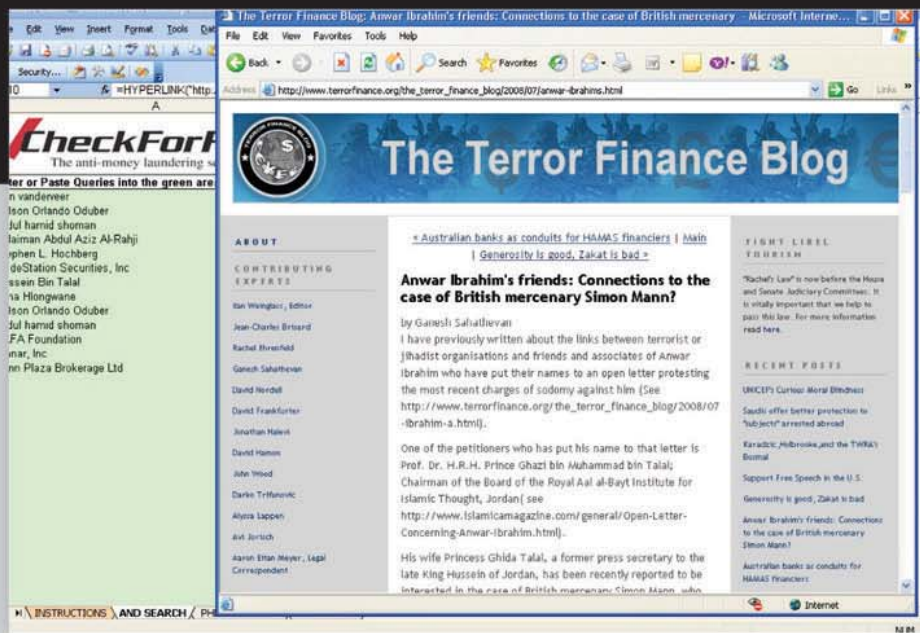


Figure 2

given to researching negative activity on entities that pose high risk or on enterprise wide internal institution lists. Searching batch files of these entities is an efficient and customizable method (see batch figure 1). The batch file research should have the utility to investigate the hit when needed, holding the hit in a live research mode. This provides for not only maximization of assets but also for obtaining the most current negative news data from the actual news document (see batch figure 2).

Where to verify the negative information collected in an inquiry

Let us assume that, during the due diligence investigation of a prospective financial institution client, the analyst finds negative information, in an article or sanctions summary, that is sufficiently serious to disqualify the individual or entity as a client or may raise the customer risk level. What does the analyst do next? There is a need to validate that information from an official source for the file, so that, should there be an audit or a question arise about the accuracy of the information, the conclusion can be supported with an official record.

The following are examples of search verification data sources in the U.S., to obtain

the evidence needed to verify the accuracy of information:

(1) Federal criminal arrests and convictions: Federal criminal cases are available online at Public Access to Court Electronic records, PACER. Visit <http://www.pacer.gov/>. Since Federal law does not allow defendants to expunge or seal records, even cases where there is no conviction remain available. Consider this a primary source of information, not merely on the subject, but his or her associates as well. Organized crime ties are sometimes discovered by looking at co-defendants, and others, linked to the subject, or in case files of the subject.

(2) State court criminal arrests and convictions: most local and county records are available online, at little or no cost. They generally do not contain the actual pleadings, like PACER does, but the analyst can still access the dockets, to verify both arrests and convictions.

(3) Information about fraud, Ponzi schemes, and other white collar crimes. Again, PACER has the details on federal crimes needed for investigations, but state court online services rarely offer the pleadings — though some do so by subscription where court filings have become paperless. Civil fraud and other white collar civil cases are

great resources on PACER. When searching for civil judgments entered against the target in state court, don't forget country records. Many attorneys routinely record certified copies in the local Official Records Index with the county, to perfect a lien on assets of the defendant. Check out the web site of the local county government for official records libraries and county public records databases.


(4) Federal Tax liens: These are also recorded in local county public records.

(5) Foreclosure judgments, final judgments and liens: Again, check official records where the target has real property.

(6) Federal securities violations or regulatory issues can be researched at the SEC web site <http://www.sec.gov/>.

(7) Sanctions: If an individual is listed as OFAC-sanctioned, in an article or other secondary source, obtain the entry at the official web site: <http://www.treasury.gov/>. Remember that there are de-listings of sanctioned parties, so always check to confirm active sanction status.

(8) Financial condition of individual or entity: Use PACER for bankruptcy filings and official records for judgments and liens from banks and other creditors.

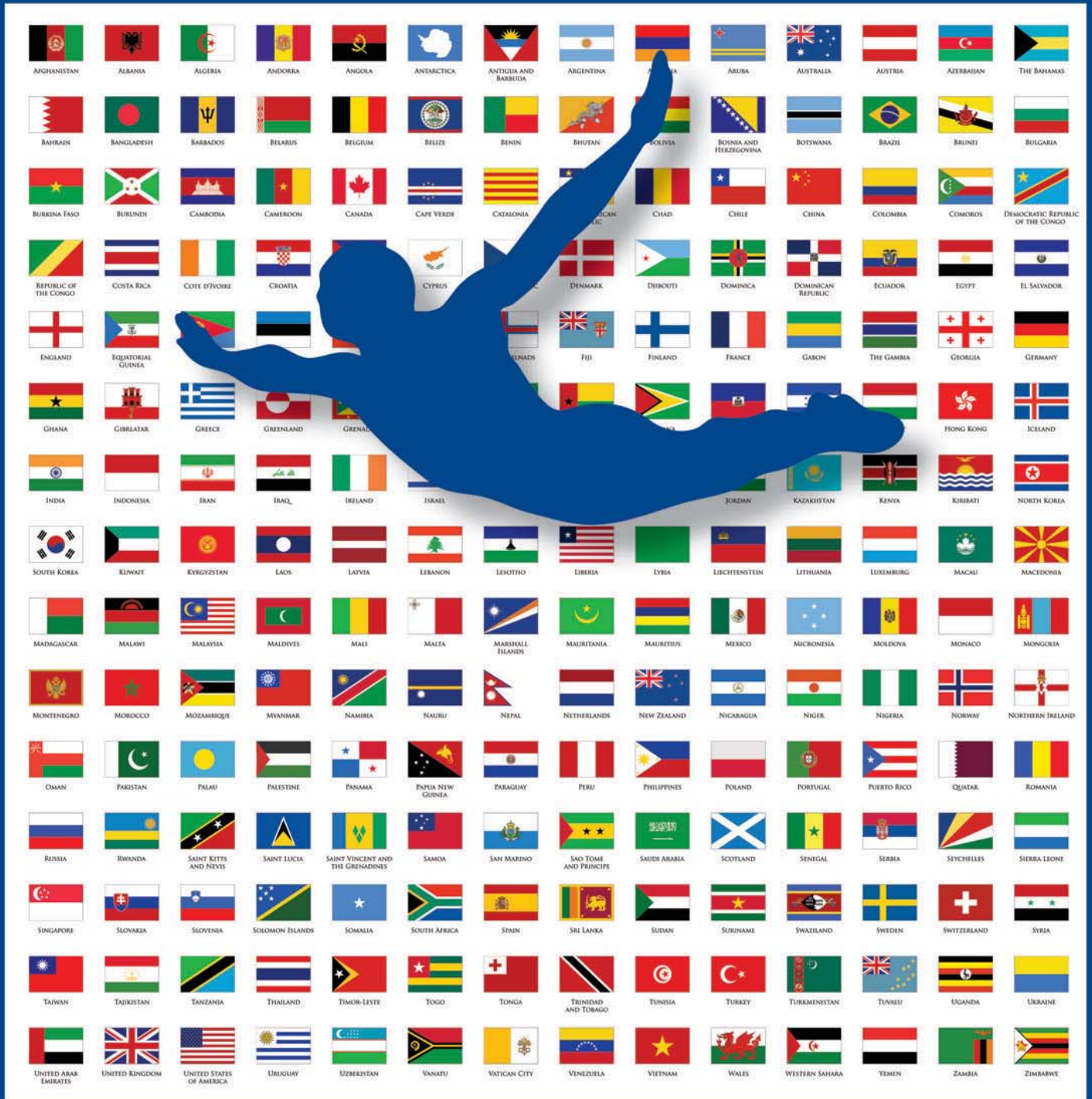
Accuracy is central when using information from negative sources. Using the foregoing resources, an analyst can validate the negative information obtained, and document not only the original information but also additional risk relevant information related to the entity with the end goal of a comprehensive profile of the entity that ensures regulatory compliance and mitigates risk. 

Robert A. Goldfinger, CAMS, CFS Cmdr. CID (retired), president, Nomino Data, USA, rgoldfinger@nominodata.com

Kenneth Rijock, financial crimes consultant, Miami, FL, USA, miamicompliance@gmail.com

A deep dive

into country risk assessment



Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and sanctions compliance risk assessments are an ongoing challenge to many financial institutions, regardless of their size or scale of operations. When institutions reach or exceed their inherent risk tolerance for offshore risk exposure and the level of risk is notably *increased* through the normal course of business, the development and implementation of a country risk assessment must be considered. Whether through business expansion, changes in customer demographic, the natural migration of customers to offshore locales, or the addition of products and service offerings to offshore customers, the country risk assessment serves as one of several key components in support of the overarching BSA/AML and sanctions risk assessment and is crucial to maintaining a sound BSA/AML and sanctions program.¹ A well-developed and documented risk-based BSA/AML risk assessment assists institutions in identifying and measuring their BSA/AML risk profile and serves as the foundation of a risk-based compliance program in support of the “four pillars” of effective BSA/AML compliance programs, which are the appointment of a BSA/AML officer, establishment of internal controls, independent testing and training.²

A well-developed and documented risk-based BSA/AML risk assessment assists institutions in identifying and measuring their BSA/AML risk profile

As a distinct subset of the BSA/AML risk assessment, the country risk assessment should use the same rating measurements and quantitative values as those used for the BSA/AML risk assessment — for example a high, medium, low or red, amber, green (RAG) score combined with numeric scores — to allow for seamless roll-up into the institution's total BSA/AML and sanctions

risk rating. Under ideal circumstances, the country risk assessment would have been developed either before or immediately at the onset of offshore exposure to the institution. However, should offshore activities be ongoing without a country risk assessment having been completed, the following information may serve to enhance the general framework used to conduct a suitable level of country due diligence necessary to establish and maintain an effective country risk assessment.

Country identification

Step one: Identify and isolate the countries of greatest potential risk to the institution. Four key datasets can be viewed as core elements of an effective country risk assessment. In order of risk category from highest to lowest:

1. Countries of known direct — or immediately anticipated — business activity; also those countries which must be considered due to significant customer influence warranting the establishment of offshore service offerings;
2. Countries of known association to the institution, particularly through counterparty, second or third-party relationships, for example indirect customers, vendors or service providers;
3. Countries identified as countries of indirect *interest* to the institution; and
4. Those remaining countries that may be deemed to have a material indirect impact on the business conducted by the institution.

Countries of known or anticipated business activity are those that require immediate risk evaluation as they present the greatest immediate risk to the institution's business operations. Should customer activity take place within these countries, the institution must ensure that effective internal controls are established to identify, measure, and monitor any resulting transaction activity that increases BSA/AML and sanctions risk exposure. Countries of known association to the institution are those through which potential offshore risk exposure may occur outside the scope of direct customer or business relationships. Whether through customer accounts with authorized users, co-borrowers, or third-party ownership/interests with offshore ties or through the use of

offshore vendors and service providers by the institution, country risk exposure should be weighed accordingly.

Those countries identified as having indirect interest to the institution may include countries whose geopolitical or economic conditions may eventually impact the institution outright or incidentally, regardless of whether it maintains a direct business presence there. Recent global geopolitical events such as the Arab Spring in the Middle East and regime changes and subtle movements in political climates such as those in Venezuela, Syria, Iran and Myanmar may affect large swaths of customers with ties to such countries that live and bank within communities served by the institution. Finally, remaining countries that may be deemed to have a material indirect impact to the institution would include those territories that may warrant monitoring should business or economic conditions develop in the near future that could escalate those countries' inherent risk to the institution to a higher level as defined in categories one through three.

Data gathering

Step two: Gather the data pertaining to countries identified as presenting risk to the institution. Numerous public resources are available to facilitate the due diligence required to build and maintain the country risk assessment, many of which are online. Public resources provide ongoing information on the geopolitical, economic and national conditions that may influence an assigned country risk score at any given time and prove to be the most cost effective risk assessment tool for any sized institution. Country due diligence information can be derived from the following categories:

1. Keystone resources, such as the Financial Action Task Force (FATFs) Non-Cooperative Countries and Territories (NCCT) list, the USA PATRIOT Act Section 311 list, and the European Union Sanctions list;
2. Official government resources and governing bodies such as the U.S. Department of State, Central Intelligence Agency (CIA), the Organization for Economic and Co-Operative Development (OECD), the International Monetary Fund (IMF), and the World Bank;

¹ BSA/AML risk assessment components include: customers, products/services, geography, and type of transactions.

² From “How Valuable is Your Risk Assessment?,” *ACAMS Today*, May 30, 2013; The FFIEC's 2010 BSA/AML Examination Manual, BSA/AML Risk Assessment — Overview, pages 22-30.

3. Third-party vendors and solutions providers such as the Economist Intelligence Unit, WorldCheck, Lexis-Nexis and Kroll Security;
4. Global media resources including the *Economist*, *Financial Times*, *New York Times*, *Wall Street Journal*, and *Washington Post*, public radio organizations such as National Public Radio.

FATF's NCCT list is the standard bearer in serving as an up-to-date risk-based resource on the regulatory regimes for most countries and jurisdictions. Similarly, though more subjective, the Section 311 and EU lists are maintained from a political perspective which considers the most recent economic and political climate news available. Official government resources and governing bodies also serve as ongoing invaluable sources of geopolitical, economic and information directly relevant to the financial climate of a given country or territory.

Third party vendors and information technology solution providers with global reach and which outsource, perform or license due diligence research for anti-money laundering and suspicious activity monitoring incorporate country risk analysis, either directly or indirectly, as a part of their service offerings or solution system product suites. If utilized, these resources can serve as potent real-time supplements to the analysis and information gathering already conducted in development of the country risk assessment. Finally, the review and use of publicly available global media resources should be a mainstay in the daily routine of any BSA/AML compliance program. Print, visual and public radio resources are additional invaluable tools that provide up-to-date advisory information on country risk conditions from a geopolitical and economic perspective. Although a more scrutinized review may be required to determine the impact of such information to institutions' business interests, resources leveraged to gather and analyze news media cannot be overlooked as part of the country risk assessment process.

Data application

Step three: Apply the data gathered through due diligence. For smaller institutions with offshore risk concerns, but lacking the human and capital resources to continually

gather and produce intelligence information, ongoing periodic government and media reviews of national and global print and visual media resources can serve as an effective foundation from which to operate. For mid-size to large institutions however, access to dedicated human and capital resources up to and including Financial Intelligence Units (FIUs) raises expectations for a high-quality risk assessment product. This is due in large part to the inherent increase in opportunities available to leverage a "full-suite" approach to due diligence initiatives using information from each of the aforementioned categories. The strategic combination of online government resources, vendor or third-party service providers, and global media resources would allow the implementation of a more robust country risk mitigation strategy. All aggregated data should finally be assessed and weighed in assigning the appropriate RAG and numeric risk score to the given country.


The methodology applied
toward maintaining a
BSA/AML risk assessment
should be viewed as
comparable to building
a business plan

The methodology applied toward maintaining a BSA/AML risk assessment should be viewed as comparable to building a business plan — the development, implementation, and maintenance of the assessment is a subjective, fluid process that requires continuous ongoing review and revision as conditions change within the marketplace. Whether as a result of changes in customer base, product and service offerings, marketing initiatives, business operation modifications, or other unforeseen circumstances, the risk assessment cannot be seen as a static endeavor. This fact is emphasized

in the FFIEC's BSA Examination Manual.³ Every consideration should be taken as to whether country risk assessment updates are required, particularly as geopolitical climates shift — which often occurs quickly.

The risk assessment maintenance schedule is the subjective choice of the institution and is directly influenced by the market/s in which it operates. Institutions may conduct an annual or more infrequent evaluation of the enterprise-wide BSA/AML and sanctions risk assessment, particularly in the case of larger multinational concerns, but a risk-based approach must always be employed. Given the unique challenges presented by country risk assessments however, a more frequent review of this specific risk component may be warranted, for example using a semi-annual cycle.

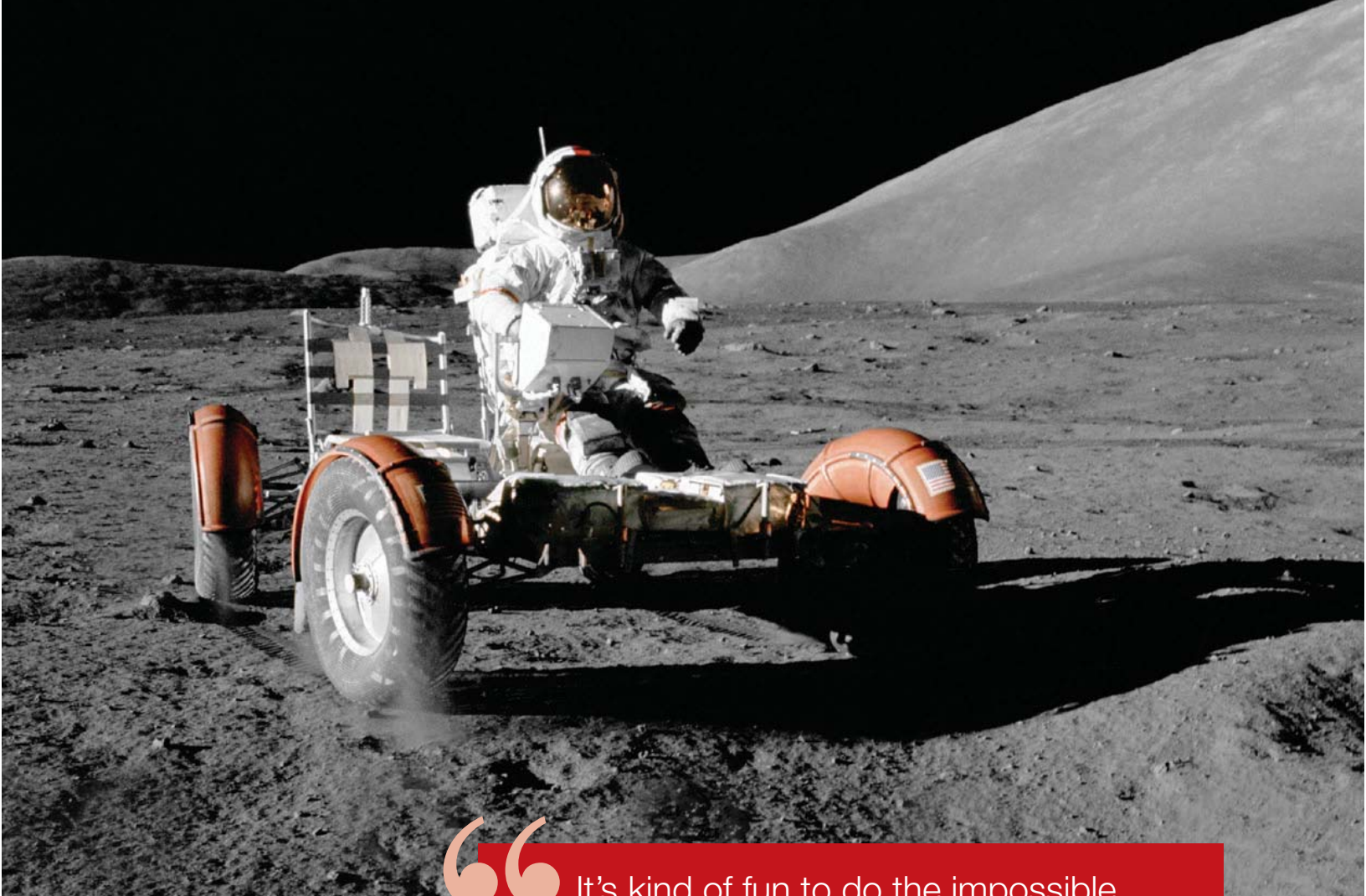
Summary

A well-developed BSA/AML and sanctions risk assessment serves to guide institutions toward identifying and vetting customers who pose the greatest risk for suspicious activities requiring more frequent and enhanced monitoring. Similarly, a well-developed country risk assessment serves to support the overarching BSA/AML and sanctions risk assessment by identifying the geographic risks faced by the institution. Smaller institutions may only afford the resources to develop a basic country risk assessment while large institutions may generally maintain the resources to construct and maintain a more complex country risk assessment that assigns risk weights to countries around the globe. Regardless of the size of the institution, compliance officers must ultimately assess and factor the country risk component should offshore financial activities occur. 

Brian Arrington, MBA, CAMS, communications director of the ACAMS Chicago Chapter, examiner with the Federal Reserve Bank of Chicago, Chicago, IL, USA, brian.arrington@chi.frb.org

The views and opinions expressed are those of the author and do not necessarily represent the views and directives of the Federal Reserve Bank of Chicago or the Federal Reserve System.

³BSA/AML risk assessment components include: customers, products/services, geography, and type of transactions.



“It’s kind of fun to do the impossible.”
— Walt Disney

With **SAFE Advanced Solutions®**, SBS helps clients do the impossible every day. Like delivering an alert hit rate of less than 0.1%.

Our patented methodology for risk ranking large databases and probabilistic alert scoring determine the severity and probability of each alert to return only the most relevant, most accurate matches. That means no mountains of low quality or false positive alerts to investigate. And more time to focus on what is important — the highest risk, most likely to be true matches.

SAFE Advanced Solutions dramatically improves the efficiency of your AML and compliance operation while mitigating risk.

Let us show you how much fun it can be to do the impossible.

Contact us at **sales@safe-banking.com** or **+1 631-547-5400**.



www.safe-banking.com

Raise your voices: We hear you

As a prosecutor leading a multi-jurisdictional suspicious activity report (SAR) review team in Central Virginia, I regularly read hundreds of SARs at a time. Our team reviews every SAR, currency transaction report (CTR), Casino SAR, and related reports that are produced in our jurisdiction and, when appropriate, either investigates the information or contacts other relevant agencies. As we review a SAR, however, I often think: “I bet the banker who wrote this SAR thinks that no one will ever read this report.”

We ARE reading your SARs. We read your SARs every day and they often play an important, if not crucial, role in investigating and prosecuting criminals. We share the information and act on the significant intelligence that you are sharing.

But what we are NOT doing is telling you about what we are doing with your SARs. It is not personal, it is just part of the business. If a citizen calls to report a drug dealer living in the neighborhood, the police usually do not call the tipster back to tell them how the investigation went. If a detective gets a tip from a patrol officer about someone who may be selling guns, the only way the patrol officer ever finds out about what happened later is by standing in the break room over coffee.

Unless you are part of a special law enforcement/private financial investigation organization, you probably never talk to the police and they probably never talk to you. But I want you to know — we read your words and treasure them. There is no better friend to the police than the tipster, the inside-source, the trustworthy citizen who shares reliable information about a potential criminal offense.

Just because you do not hear about the results does not mean we are not listening. That tip about the old man sending money to a suspicious jurisdiction? We met with him and told his children the story that he told us about the mysterious woman with whom he has a love affair to whom he is sending tens of thousands of dollars. That tip about the man running a suspicious stock scheme?

Turns out we already knew he was stealing from his company and locked him up quickly once we heard your tip. That tip about the young man sending thousands of dollars through a stored value card to Miami? We had suspected he was selling drugs and your tip helped us figure out who his connection was.

Just because we do not prosecute a person for the crime you told us about does not mean your SAR did not help protect the community. You might have warned us about criminal structuring, but the real crime might have been drug dealing. You might have warned us about tax evasion, but the real crime might have been embezzlement. You might have warned us about someone moving money to evade export regulations, but the real crime might have been bribing government officials. You may only ever see part of the whole picture, but you helped us finish the portrait and see the truth.


I remember a SAR we received about a woman who we knew was connected to a guy at the top of a large criminal scheme. The SAR related how she moved a large amount of money in a very suspicious manner, but never mentioned the man because he was not involved in the transactions — or so the financial institution thought. We suspected otherwise, however, and our investigation led straight back to him. But I bet to this day, because nothing happened to the woman, the SAR writer thinks that we never even cared about or read the report.

It is common for us to see SARs that report women moving money in strange ways and recognize the women as girlfriends or associates of known criminals. It is also common for us to see SARs that report odd behavior that appears to have no explanation and recognize the importance of the behavior in the context of other intelligence. There is no way for a SAR writer to know what we know. But there is also no way for us to know what you know. That is why the SAR process is so valuable. Of course, we can almost never share our knowledge with you.



We read every SAR in our jurisdiction because we know many of our bad guys by name. We are a small jurisdiction and often know if there is already an investigation on someone you report to us. Sometimes, however, you tell us something that we did not know. When we look under the rock you pointed out to us in your SAR, we never know what we will find, and sometimes it is something neither of us expected. More than once we have been surprised to find that a so-called upstanding citizen was in fact a criminal, a thief or a fraudster.

So please continue to speak up. But don't forget that SARs are not the only way to communicate with law enforcement. When money shows up that smells like marijuana, or has white powder residue on it, call us! We can come and test it on the scene. When someone appears showing false identification to cash an obviously stolen check, get law enforcement on the scene. When you suspect that someone is exploiting an elderly client, you are permitted to call the police to report the crime. In these cases, nothing beats a quick response, and SARs have an inevitable delay.

Lastly, remember that it is not enough to speak loudly — you also have to speak clearly. I might have learned to speak banker, but a detective who just finished eight years of driving a radio car on midnight shift does not speak your language. He wants very much to hear what you have to say. And I guarantee that he appreciates your work. Just don't expect him to say thank you. You'll have to settle for me saying it: Thank you. 

Elliott Casey, assistant commonwealth's attorney, special assistant United States attorney, Albemarle County, VA, USA, ecasey@albemarle.org

ENFORCEMENTS ARE WIDESPREAD... STEER CLEAR OF THE HEADLINES

Transaction Monitoring
Customer Due Diligence
FATCA
Sanctions Screening
Model Risk Management



HOW EFFECTIVE IS YOUR AML PROGRAM?

NICE Actimize provides comprehensive, proven AML solutions that proactively uncover money laundering activity and enforce compliance across the enterprise.

To ensure effective compliance and future-proof your business, visit www.niceactimize.com/acams2013

NICE ■ ACTIMIZE

Old MacDonald of sanctions compliance and customer due diligence



If you are keeping score, it seems that sanctions compliance is a bit like the old nursery rhyme *Old MacDonald Had a Farm*. You know, “here a sanction, there a sanction, everywhere a sanction-sanction...”

Members of the anti-money laundering (AML) and sanctions compliance community should be aware of the economic sanctions programs put in place by the United States government. These programs are designed with two purposes. First to identify bad actors who are affiliated with rogue political regimes or with other individuals or organizations that are involved in all sorts of nefarious endeavors — including but not limited to — narcotics trafficking, transnational organized crime, terrorist organizations or the proliferation of weapons of mass destruction. Second they are designed to penalize those who enable business with those sanctioned entities. The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) administers most of these sanctions programs. In recent years, the OFAC Specially Designated Nationals (SDN) List alone has averaged somewhere in excess of 70 updates annually. This is not even

touching on the compliance universe represented by export control regulations, other U.S. government sanctions programs, or sanctions programs from other jurisdictions.

The U.S. government has long sought to choke off funding to regimes, organizations and individuals that represent threats to U.S. interests, including Iran, Cuba and Syria, via enforcement of U.S. sanctions programs. Through record penalties and aggressive enforcement over the past several years, OFAC has tried to make the point crystal clear that enabling these bad actors, whether by intent or by circumstance, is simply not acceptable and is definitely not in anyone’s best interest.

Sanctions laws and regulations, such as those promulgated by OFAC, have garnered considerable attention over the past several years, through major regulatory actions against global financial institutions including HSBC, Standard Chartered Bank, ING and Bank of Tokyo-Mitsubishi for violations of sanctions laws. Civil money penalties assessed against these four institutions ranged from US\$258 million to \$1.92 billion each — certainly

attention getters — and examples of due diligence and process failures. Those institutions will certainly not be the last to run afoul of OFAC’s regulations. This is especially true as there are conflicting laws in other jurisdictions that appear to directly clash with U.S. Treasury’s regulations, thereby creating yet another “wrinkle” in the global sanctions compliance world.

Sanctions compliance is not for the faint of heart. While OFAC sanctions continue to grab headlines and advance the U.S. government’s foreign policy agenda with well-publicized enforcement actions, other countries and regulatory bodies, including the United Kingdom, European Union and the United Nations, along with more than 60-plus other countries, have some sort of sanctions programs in place. This, to say the least, makes sanctions compliance a much greater challenge for both corporate and financial organizations. Compliance officers reading this are all too familiar with the anxiety that complexities of such regulations can bring to the forefront.

Knowledge of various sanctions programs and their intricate gradations is simply not enough. Understanding the art and science of exactly what data to examine, and when and how it should be examined is absolutely critical to success within the sanctions compliance process. Demonstrating a thorough grasp of the nuances of how filtering or screening processes function and knowing how to adjust aspects of the screening process, along with knowing what to do to verify or validate the match and how to perform necessary due diligence related to such matched entities, is equally vital to your success in making the screening process genuinely productive.

While corporations and financial institutions are contending with the ever-changing landscape of sanctions regimes both at home and abroad, and the increasingly “creative” measures that countries like Iran are employing to evade sanctions, the dawn of U.S. state-level sanction programs add even more complexity to the process; and may well increase your risks of heartburn as an unexpected consequence.

In recent years, the U.S. Congress has enacted legislation authorizing states to prohibit investments in, or divest assets from, Sudan and Iran. The Sudan Accountability and Divestment Act of 2007 authorizes states and local governments to adopt divestment or investment prohibition measures involving: (1) persons within state or local government determined to be conducting business operations in the Sudanese energy and military equipment sectors or (2) persons having a direct investment in or carrying on a trade or business with Sudanese entities or the Government of Sudan, provided certain notification requirements are met.

The Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) which was enacted in 2010, includes provisions authorizing state and local governments to divest from those businesses making investments of US\$20 million or more in Iran’s energy sector after adequate investigation and notification have occurred. Both laws stipulate that a measure falling within the scope of the authorization is not pre-empted by any federal law or regulation.

So far more than two dozen U.S. state governments have, with much less fanfare than their federal brethren, implemented their own various sanctions laws, which are designed to prohibit state procurement as well as investment with companies doing business with certain countries or other entities that

are under the scrutiny of sanctions by the U.S. government. Such laws are referred to as “divestment sanctions.”

Increasingly state governments are penalizing parties for doing business with companies who in turn are doing business with sanctioned countries or prohibited parties. With the addition of such state-level laws, overall sanctions compliance can be more difficult than solving the Rubik’s Cube puzzle while being blindfolded.

Another point of consternation and angst involves exactly how such state scrutinized organization lists are actually assembled and maintained. Frequently, such state lists may likely diverge from OFAC’s List of Specially Designated List of Sanctioned Entities and Blocked Persons. Many business associations and others in the know have argued that state agencies lack the time, funding and subject-matter expertise to properly and accurately compile and maintain information on companies with business ties to sanctioned countries or entities. Without the resources and the interagency ties that OFAC has access to, states must rely upon open-source information obtained from news and media outlets, advocacy groups or other sources. The problem here is potentially one of informational quality concerning the targeted entity.

The advent of state sanction programs leaves financial institutions and other corporations to screen an ever-growing number of sanctions lists, adding yet another compliance headache to a field that seems to have no lack of them already. More information on state sanctions programs from the various state governments themselves may be found on various state government web sites, as well as the following site: <http://www.fas.org/sgp/crs/misc/RL33948.pdf>

Perhaps this discussion will spark both thought and action, not only about state sanctions list but also about the efficacy of your entire sanctions compliance program. When is the last time *your* organization had a truly independent review of your sanctions compliance program from top to bottom to make sure that your policies, procedures, information technology processes and day-to-day business operations are all fully aligned to meet your regulatory compliance needs in the *best manner possible*? If the answer is never, which happens much more often than many might admit, or if the answer is not for a while, then perhaps now is the proper time to take a look at these processes.

To be sure, there are a host of risks associated with doing business with bad actors that go beyond the scope of nationally or state sanctions programs. There are an equal number of risks associated with a program that may have the appearances of working well at first glance, but is off by “just a little” when the veneer is peeled back more closely for examination. But it is interesting to note that of the US\$3.5 billion in civil money penalties assessed over the past 12-18 months by U.S. regulatory authorities, the largest penalty assessments all have sanctions program failures as core components of their regulatory issues.

Unfortunately, a good number of organizations have varying degrees of flaws in their sanctions compliance programs, but are happy “whistling by the compliance graveyard” because they have not been penalized for a program failure thus far. Often, the response to this suggestion is something like: “Thank you, but we have sound sanctions compliance policies in place.” We all know that effective policies are one thing, but that implementation of proper, effective procedures is often another thing entirely.

If you were to ask any of the financial institutions that have recently been the recipients of civil money penalties whether they had sound policies in place, my guess is that their initial answer would be yes. The problem may not be policies but rather making sure the proper framework for execution of valid procedures is effectively in place. The next logical question seems to be: “What can I do about it?”

So...take a deep breath and take some time to make sure your sanctions compliance program and the related business processes that you have implemented are up to par in meeting sanctions regulations requirements associated with applicable state, national and international sanctions programs. An independent review and test of your program by parties who can look at your program in a truly objective manner might just be the next right move. A little proactive work on your part now can yield greater benefits and peace of mind within your organization tomorrow. **A**

Shaun M. Hassett, CAMS, CDDP, independent regulatory compliance consultant and advisor, Financial Evaluations and Examinations and International Management Advisory Group, Algonquin, IL, USA, proper.due.diligence@gmail.com

Mexico's security threat: Organized crime and money laundering

Mexico is seen as one of Latin America's most promising countries with ambitions to become a regional economic leader. According to a Germany Trade & Investment (GTAI) report published by Germany's economic development agency, Mexico will see growth of 3.5 percent for the year 2013.

Averaging between US\$320 and US\$340 billion, Mexico alternates with China as America's second largest trading partner; however, not only for legitimate trade. According to a report published by Chatham House in November 2012 titled: *Organized Crime, Illicit Drugs and Money Laundering: the United States and Mexico*, Mexico has become the number one provider of illicit drugs to the United States. Furthermore, Mexico fell negatively in Transparency International's corruption perception index to 105th place in 2012 from 57th in 2002. According to an article published by *Reuters* the amount of illegal funds laundered in Mexico on a yearly basis ranges from US\$ 10 billion to US\$ 45 billion. The laundered funds are seen as the main driver of the growing violence in the country, which like other countries in Latin America has seen a dramatic increase in violence in recent years.¹

Given this background, it is clear that the country's potential to continue its path of economic growth and development is threatened by corruption, organized crime, government bureaucracy and the lack of trust in the country's police forces as reported in the Global Competitiveness Report issued by the World Economic Forum 2012-2013. This article sets out some of the crime and security threats currently facing Mexico and measures undertaken to deal with these issues.

Regional crime structures and overlapping criminal networks

Since June 2008, the *Los Angeles Times* has published reports by journalists based on both sides of the border between Mexico and



the United States reporting upon the violent struggle amongst Mexican drug cartels for control over the lucrative drug trade to the United States. According to the newspaper blog titled: *Mexico Under Siege, the Drug War at Our Doorstep* the conflict as it is termed, has left thousands dead, paralyzed whole cities with fear, and spawned a culture of corruption reaching the upper levels of the Mexican state.²

A report published by the Woodrow Wilson International Center (Wilson Center), claims that over 47,000 people were killed in crime related violence in Mexico in the five years leading up to the election in 2012.³ The Wilson Center's Mexico Institute claims that a number of important new hypothesis and assumptions have begun to emerge about the nature and extent of the security threats

posed by organized crime and violence in Mexico. In particular the breakdown in the one-party political system and the arrival of multi-party political competition has contributed to a regionalization of criminal activity. State governments and municipalities have less capacity to bring criminal activity under control, or re-establish equilibrium within the illegal market. Rather than centrally organized cartels, traffickers appear to be organized primarily as a series of overlapping networks that at times work together and at other times operate independently or compete with each other. Mexico's domestic criminal markets tend to be decentralized, more competitive and, as a result, more violent. Alejandro Hope's *Taxonomy of Criminal Groups*⁴ (see diagram on next page) sets out the areas of activity and reach of Mexico's organized crime groups.

¹ Mexico's overall homicide rate (18 per 100,000 inhabitants) is uncomfortably high, but pales in comparison to Honduras (82), El Salvador (66), Venezuela (49), Belize (41), and Guatemala (41), Colombia (33), the Bahamas (28), Brazil (22), and the U.S. territory of Puerto Rico (26) - <http://justiceinmexico.files.wordpress.com/2012/03/2012-tbi-drugviolence.pdf>

² <http://projects.latimes.com/mexico-drug-war/-/its-a-war>

³ <http://www.wilsoncenter.org/publication/considering-new-strategies-for-confronting-organized-crime-mexico>

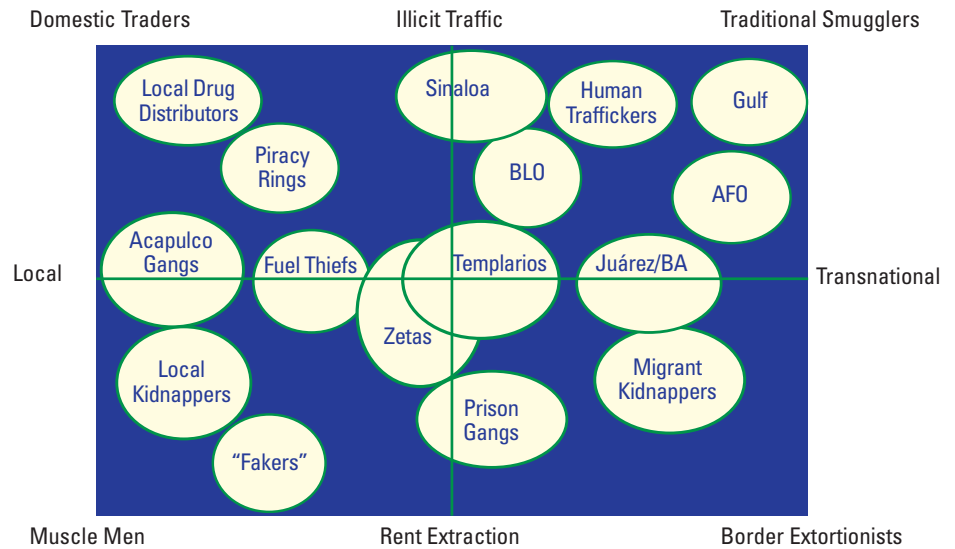
⁴ http://www.wilsoncenter.org/sites/default/files/Alejandro_Hope_0.pdf

The Mexican drug war

The Mexican Drug War is an ongoing armed conflict among rival drug cartels striving for regional control. While it is thought that many factors have contributed to the escalating violence in Mexico, security analysts in Mexico City trace the origins conflict to the unraveling of a long-time implicit arrangement between narcotics traffickers and governments controlled by the Institutional Revolutionary Party (PRI). This is particularly interesting given PRI's comeback to power in 2012.

According to the academic, David J. Danelo, the situation in Mexico is often compared to that in Colombia. He underlines however, that unlike the FARC in Colombia, Mexico's drug cartels have no desire to reshape their country in accordance with Marxist ideology. Mexico's narcotics groups have reportedly more in common with Somali pirates than Colombian rebels: Both groups seek to create anarchy so they can exploit the defenseless and dominate local markets. Like Somali pirates in East Africa's coastal villages, Los Zetas have thrived in stateless voids, stealing money from merchants and becoming minor celebrities within their respective regions. While Colombia faced a political insurgency, Mexico confronts something like land piracy led by powerful drug kingpins.⁵

As reported by *STRATFOR*, the demise of the Guadalajara cartel in the late 1980s, which controlled drug trade routes into the United States through most of Mexico, has seen Mexican cartels fracturing into more geographically compact, regional crime networks.⁶ This trend has continued for more than two decades and has impacted all of the major cartel groups in Mexico. Although Mexican drug cartels, or drug trafficking organizations, have existed for several decades, they have become more powerful since the demise of Colombia's Cali and Medellín cartels in the 1990s. Mexican drug cartels now dominate the wholesale illicit drug market, controlling 90 percent of the cocaine that enters the United States. Arrests of key cartel leaders, particularly in the Tijuana and Gulf cartels, have led to



Source: Alejandro Hope

increasing drug violence as cartels fight for control of the trafficking routes into the United States.⁷ Sinaloa Federation and Los Zetas are currently the most powerful cartels in Mexico.

According to the U.S. National Drug Intelligence Center, major Mexican-based Transnational Criminal Organizations (TCO) and their associates are solidifying their dominance of the U.S. wholesale drug trade and will maintain their reign for the foreseeable future. Their pre-eminence derives from a competitive advantage based on several factors, including access to and control of smuggling routes across the U.S. border and the capacity to produce (or obtain), transport, and distribute nearly every major illicit drug of abuse in the United States.⁸ These TCOs are extremely well funded and well-armed — and they are presenting a formidable threat to the security, prosperity, and psyche of the people of Mexico and the United States. Illegal drug export revenues from Mexico in 2011 were estimated at approximately US\$6.2 billion, comprised of the major drugs: cocaine (est. US\$2.8bn), followed by marijuana (US\$1.9bn), heroin (US\$0.9bn) and methamphetamines (US\$0.6bn).⁹ Although both the governments of the U.S. and Mexico recognize that they must attack the economic

power of transnational criminal organizations to weaken them the challenges faced are tremendous.

Anti-money laundering efforts in Mexico

Celina B. Realuyo, assistant professor of National Security Affairs at William J. Perry Center for Hemispheric Defense Studies at National Defense University, underlined in a report published by the Wilson Center in May 2012, the importance of anti-money laundering efforts in tackling organized crime in Mexico and alleviating the security threat emerging as a result of the activities carried out by organized crime networks.¹⁰

Former President Felipe Calderon also recognized the importance of preventing money laundering and combating financial terrorism as part of the state's strategy against organized crime. Calderon proposed a law in 2010 to crack down on money laundering in a bid to attack the finances of the country's powerful drug cartels.¹¹ On 11 October 2012, Mexico's senate approved the modifications to the anti-money laundering law introduced by the executive in August 2010 and the current President Enrique Peña Nieto signed the bill into law on 16 October 2012, which came into force in July 2013.¹² The new legislation obliges designated

⁵ https://www.fpri.org/docs/Toward_a_US_Mexico_Security_Strategy_Danelo.pdf

⁶ <http://www.stratfor.com/weekly/mexicos-drug-war-balkanization-leads-regional-challenges>

⁷ https://en.wikipedia.org/wiki/Mexican_Drug_War

⁸ <http://www.justice.gov/archive/ndic/pubs44/44849/44849p.pdf>

⁹ <http://www.wilsoncenter.org/publication/considering-new-strategies-for-confronting-organized-crime-mexico>

¹⁰ http://www.wilsoncenter.org/sites/default/files/Realuyo_U.S.-Mexico_Money_Laundering_0.pdf

¹¹ <http://uk.reuters.com/article/2012/10/11/uk-mexico-drugs-idUKBRE89A1PX20121011>

¹² <http://www.gtlaw.com/News-Events/Publications/Alerts/165136/An-Overview-of-Mexicos-New-Anti-Money-Laundering-Law>

non-financial businesses and professions (DNFBP) to identify their clients and report suspicious operations or transactions above designated thresholds to the Secretariat of Finance. The thresholds vary by sector. The legislation establishes a Specialized Financial Analysis Unit in the Office of the Attorney General; restricts cash operations in Mexican pesos, foreign currencies and precious metals for a variety of “vulnerable” activities; and imposes criminal sanctions and administrative fines on violators of the new legislation. Under the above regulations, casinos, notaries, lawyers, accountants, jewelers, realtors, non-profit organizations, armored car transport companies, armored services, construction companies, art dealers and appraisers, and non-bank institutions providing credit card, pre-paid card, or traveler check services will also be subject to know your customer (KYC) and suspicious transaction report (STR) requirements.¹³ An article published by *Reuters* on 12 October 2012 highlighted that the federal law puts restrictions on cash purchases of real estate, jewelry, armored cars and other assets that criminals use to launder illicit funds and that companies are required to report large cash purchases namely car sales of more than 200,000 pesos (about US\$16,000) and real estate purchases of more than 500,000 pesos (about US\$39,000).¹⁴

The Mexican security threat — efforts and reforms

Despite fears that Mexico would return to being an authoritarian regime following the election of Enrique Peña Nieto as president in 2012 reinstating the Institutional Revolutionary Party (PRI), which had run the country for 70 years, prior to the former regime which held power for twelve years until 2012, Mexico's current government has been praised for having pushed on with long awaited reforms.

According to a report published by *STRATFOR*, Nieto's most significant initiative is his plan to consolidate and restructure federal law enforcement in Mexico. Pena Nieto's ruling Institutional Revolutionary Party has introduced legislation that would switch oversight of the federal police, among other entities, away from the Public Security Secretariat to the Interior Ministry. The president also announced plans to bring the state

police from each of Mexico's 31 states under a unified federal command. In December 2012, Mexico announced that it would deploy a new 10,000-member security force to regions of Mexico where violence and instability are greatest. Until the new force was set up, the military would remain in the streets in an effort to maintain order. The federal police were to add 15 units that will focus solely on kidnapping and extortion.


Furthermore, in May 2013, Nieto announced the creation of an investigative task force to search for thousands of missing Mexicans in response to anguished families and mothers on a hunger strike. The new effort is part of an effort to whittle down a list of more than 26,000 people who were reported missing, many seized by drug traffickers or by state security forces, during the Calderon presidency.¹⁵

The private sector has also played a remarkable role in dealing with organized crime and the resulting violence in Mexico. Various reports published by the *Economist* in June 2013 portray the private sector initiatives, in particular those in Mexico's industrial cities which are engaged in reducing violence and contributing to programs to alleviate some of the roots of organized crime in Mexico. The article reported that the private sector has helped the government, with both money and technical expertise, to recruit and run a new police force. The first task was to purge state and local police of infiltration by drug mafias. Rodrigo Medina, governor of the state of Nuevo León of which Monterrey — Mexico's biggest industrial city — is the capital city, says 4,200 police were fired or jailed after failing the lie-detector and other tests. At first, the armed forces (mainly marines) were drafted to keep order. Then, with advice from the human-resources departments of Monterrey's biggest firms, the government launched a national recruitment drive to build a new state police force, known as Fuerza Civil (civil force). Although it is in its early days the project seems to have been successful and most importantly enjoyed the trust of the citizens.

Conclusion

According to an article published in the *New York Times* in June 2013, Mexico is undergoing increased scrutiny from NGOs and the local media as well as opposition parties who

challenge and expose the faults of the status quo and increasingly seeking to hold officials accountable.¹⁶ Freedom of information laws, recent legislative overhauls demanding more accountability from state governments and an increasingly technologically engaged society have been more successful in preventing murky finances from going unquestioned. As a result, tales of disgraced former governors are coming to surface and being made public. The culture and mentality of “El que no tranza, no avanza,” or “He who does not cheat, does not get ahead,” a popular Mexican motto, reportedly still remains. According to the same article legal prosecution and enforcement remain an issue in Mexico, as the country has yet to find an effective mechanism to translate citizen participation into structural change. In summary however, naming and shaming is becoming common practice.

From a security perspective and as pointed out by David J. Danelo in a report published by the U.S. Foreign Policy Research Institute in February 2011, no relationship in the Western Hemisphere is fraught with more geopolitical complexity than the one between Mexico and the United States.¹⁷ The two nations are both partners and competitors. Given the economic, social and cultural rivalries, security partnerships between the United States and Mexico have been difficult to create. Failure to build capacity and structure partnerships will enhance the strength of drug cartels and fuel instability and violence. Although serious challenges do however remain, some success stories do exist. Baja California's turnaround and stabilization from one of Mexico's most violent to one of its safest, represents a strategic success story. Within the context of this reality and knowing that the proceeds of crime enrich and empower transnational criminal organizations and allow them to undermine state institutions and economic prosperity, financial institutions and their AML officers dealing with Mexico-related transactions do have a key role to play alongside other private sector initiatives in delivering a sustainable future to the Mexican state. 

Jennifer Hanley-Giersch, CAMS, managing director, Business Risk Research Limited, Berlin, Germany, jennifer.hanley@business-risk-research.com

¹³ <http://www.knowyourcountry.com/mexico1111.html>

¹⁴ <http://uk.reuters.com/article/2012/10/11/uk-mexico-drugs-idUKBRE89A1PX20121011>

¹⁵ <http://www.latimes.com/news/nationworld/world/la-fg-mexico-numbers-20130528,0,614114.story>

¹⁶ http://www.nytimes.com/2013/06/24/world/americas/official-corruption-in-mexico-once-rarely-exposed-is-starting-to-come-to-light.html?pagewanted=2&_r=2&hp

¹⁷ https://www.fpri.org/docs/Toward_a_US_Mexico_Security_Strategy_Danelo.pdf

Does OFAC have you chasing your tail or do you sit in command?



**Technology can change behavior—and performance
—when it comes to watch list screening.**

OFAC and other watch lists change constantly, leaving you running in circles to keep up. Let CSI be your new best friend when it comes to regulatory compliance. With WatchDOG® Elite, we offer an advanced watch list screening solution that simplifies every day operations and regulatory exams. Our feature-rich solution delivers unified search and reporting options, streamlined review and resolve functionality, and master search capabilities, taking the bite out of your OFAC compliance obligations.

Learn more about CSI's best-of-breed solutions.

compliance.csiweb.com



Formerly **ATTUS** Technologies, Inc.



Core Bank Processing • Managed Services • Mobile & Internet Solutions
Payments Processing • Electronic & Print Distribution • Regulatory Compliance

888.494.8449
compliance.csiweb.com

CANADA 2013: The fight against financial crime continues



It has been a couple of years since I wrote on the landscape in Canada. Over the last several months Canadians have been shown example after example of allegations of corrupt activities. The Province of Quebec has finally come to terms with organized crime's influence in the construction industry. Flowing from the Charbonneau Commission, testimony has revealed just how pervasive the influence of organized crime was on the political scene.

Most recently Canadians have had almost nightly news broadcasts pertaining to four senators, three of whom have had an RCMP

investigation launched against them for breach of trust. The investigation pertains to their alleged fraudulent filing of personal expenses, from housing allowances to travel. These false expense claims have amounted to tens of thousands of dollars. The fourth senator has yet to be investigated by the RCMP, but as of August 12, 2013 the external auditor has confirmed similar breaches as to the other three senators. The allegations are calling into question the validity of the Canadian Senate.

If we look at the current landscape in Canada relative to our progress in combatting money laundering and terrorist financing a recent Senate report, which in my view was one of the most objective reports coming from the Senate in recent memory, has highlighted some real deficiencies in Canada's overall AML/CTF strategy. The Senate report in March of this year titled: "Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not Really," sent a clear message that we all

need to become more effective and work together. The report summarized their findings as follows:

Summary of Recommendations:

The Desired Structure and Performance

1. The federal government established a supervisory body, led by the Department of Finance, with a dual mandate:

- To develop and share strategies and priorities for combatting money laundering and terrorist financing in Canada; and
- To ensure that Canada implements any recommendations by the Financial Action Task Force on Money Laundering that are appropriate to Canadian circumstances. This supervisory body should be comprised of representatives of federal interdepartmental working groups and other relevant bodies involved in combatting money laundering and terrorist financing.

Commentary: The recommendations focus on the need to have governmental agencies — inclusive of regulatory and enforcement — become better at working together and ensuring ongoing dialogue.

2. The federal government requires the supervisory body recommended earlier to report to Parliament annually, through the Minister of Finance, the following aspects of Canada's anti-money laundering and anti-terrorist financing regime:

- The number of investigations, prosecutions and convictions;
- The amount seized in relation to investigations, prosecutions and convictions;
- The extent to which case disclosures by the Financial Transactions and Reports Analysis Centre of Canada were used in these investigations, prosecutions and convictions; and
- Total expenditures by each federal department and agency in combatting money laundering and terrorist financing.

Commentary: This recommendation is music to my ears since I have advocated for years that the success of any AML/CTF program has to be based on prosecutions, forfeitures and convictions. Simply relying on the amount of reports sent to enforcement agencies by FIUs is analogous to building a car and forgetting the engine.

3. The federal government ensures that, every five years, an independent performance review of Canada's anti-money laundering and anti-terrorist financing regime,

and its objectives, occurs. The review could be similar to the 10-year external review of the regime conducted in 2010, and could be undertaken by the Office of the Auditor General of Canada. The first independent performance review should occur no later than 2014.

Commentary: This conforms to recommendations of FATF but to be of value the government needs to ensure that any audits are carried out by appropriate subject-matter experts who have the requisite skills, background and knowledge to objectively assess an AML/CTF program. Too often these reviews are carried out by companies with a strong lobby to the government.

4. The federal government considers the feasibility of establishing a fund, to be managed by the supervisory body recommended earlier, into which forfeited proceeds of money laundering and terrorist financing could be placed. These amounts could supplement resources allocated to investigating and prosecuting money laundering and terrorist financing activities. The government should ensure that implementation of this recommendation does not preclude victims from collecting damages awarded to them by a court of law in a suit brought under the *Justice for Victims of Terrorism Act*.

Commentary: In my view this establishes a good balance between direct payment to investigating agencies and having the funds simply disappearing into the Canadian Government's overall revenue process.

5. The federal government ensures that the Financial Transactions and Reports Analysis Centre of Canada and the Royal Canadian Mounted Police employ specialists in financial crimes, and provide them with ongoing training to ensure that their skills evolve as technological advancements occur.

Commentary: I have been arguing this point for years. All of us in the industry realize that expertise is essential to be able to effectively and efficiently carry out responsibilities under the PCMLTFA. This will require fundamental changes within the RCMP and FINTRAC's staffing and promotion processes and will only be successful if there is some form of skill based pay.

The Appropriate Balance Between the Sharing of Information and the Protection of Personal Information

6. The federal government requires the Royal Canadian Mounted Police, the Canadian Security and Intelligence Service, the

Canada Border Services Agency and the Canada Revenue Agency to provide quarterly feedback to the Financial Transactions and Reports Analysis Centre of Canada regarding the manner in which they use case disclosures and how those disclosures could be improved.

7. The federal government permits the Financial Transactions and Reports Analysis Centre of Canada to provide case disclosures in relation to offences under the *Criminal Code* or other Canadian legislation.

8. The federal government develops a mechanism by which the Royal Canadian Mounted Police, the Canadian Security and Intelligence Service, the Canada Border Services Agency and the Canada Revenue Agency could directly access the Financial Transactions and Reports Analysis Centre of Canada's database. The Privacy Commissioner of Canada should be involved in developing guidelines for access.

9. The federal government and the Financial Transactions and Reports Analysis Centre of Canada, in consultation with entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations, annually review ways in which:

- The compliance burden on reporting entities could be minimized; and
- The utility of reports submitted by reporting entities could be optimized.

10. The Financial Transactions and Reports Analysis Centre of Canada provide entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations with:

- On a quarterly basis and specific to each entity, feedback on the usefulness of its reports;
- On a quarterly basis and specific to each sector, information about trends in money laundering and terrorist financing activities; and
- Tools, resources and other ongoing support designed to enhance the training of employees of reporting entities in relation to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its obligations.

Commentary: Recommendations 9 and 10 establish the mandate for FINTRAC to provide feedback to reporting agencies and to consider their concerns relative to the costs and resource intensiveness of complying with the regulations.

11. The Financial Transactions and Report Analysis Centre of Canada review its guidelines in relation to the period in which reports must be submitted to it by entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations. The goal of the review should be to ensure that, to the greatest extent possible, reports are submitted in “real time.”

12. The federal government, notwithstanding the recently proposed changes to Canada's *Witness Protection Program Act*, ensures that the safety of witnesses and other persons who assist in the investigation and prosecution of money laundering and/or terrorist financing activities is protected.

13. The federal government establishes a mechanism by which employees of entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations, and other individuals, could anonymously notify the Financial Transactions and Reports Analysis Centre of Canada about:

- Failures to comply with the requirements of the Act; and
- Individuals or entities possibly complicit in money laundering and/or terrorist financing. (p. 17)

The Optimal Scope and Focus

14. The federal government enhances Canada's existing anti-money laundering and anti-terrorist financing regime by placing additional emphasis on:

- The strategic collection of information; and
- Risk-based analysis and reporting.

15. The federal government review, on an ongoing basis, the entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations to ensure the inclusion of sectors where cash payments exceeding the current \$10,000 threshold are made. (p. 19)

16. The federal government eliminates the current \$10,000 reporting threshold in relation to international electronic funds transfers.

17. The federal government review annually, and update as required, the definition of “monetary instruments” in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* in order to ensure that it reflects new payment methods and technological changes.

18. The federal government, in consultation with the proposed Financial Literacy Leader, develops a public awareness program about Canada's anti-money laundering and anti-terrorist financing regime, and about actions that individuals and businesses can take to combat money laundering and terrorist financing.

Overall comments:

This aforementioned findings highlight the need for having ongoing professional training and networking opportunities with all professions tasked with thwarting money laundering and terrorist financing. By creating ACAMS Chapters we create a recognizable vehicle that provides a framework and ongoing opportunities for our colleagues in Canada. We all know the emphasis placed by regulators on the need for ongoing training and therefore having a network of like-minded professionals from all sectors affords a venue for best practice sharing, money laundering and terrorist financing trend updates, and the benefit of having a collaboration of experts to assist us in achieving new regulatory changes.

What has been accomplished?

Over the course of the past year Canada has forged ahead with the establishment of a vibrant Vancouver Chapter and a soon to be launched Montreal Chapter. Vancouver's executive board hit the ground running with a group of motivated and professional money laundering practitioners who have embraced the need to be able to organize networking and learning events under the ACAMS umbrella. The formation of this chapter serves to enable ACAMS members on the west coast to capitalize on the value of sharing best practices and discussing current issues confronting the financial sector. The goal is to ensure that regulators, law enforcement and representatives from all areas of the financial sector collaborate with the goal of thwarting criminal money laundering and terrorist financing.

Montreal's entry into the chapter family will add a whole new dimension to ACAMS since the membership in Quebec wants to establish a French language ability that will be viewed positively, initially in Canada and then spread to other French speaking countries. Under the leadership of Sylvain Perreault from Desjardins, who helped select a phenomenal team, I am proud to say that Montreal is well on its way in setting a high standard with very laudable goals.


The Canadian Chapter which will be renamed as the Greater Toronto Chapter and has continued to provide learning and networking opportunities for Canadian ACAMS members. My co-chair Karim Rajwani from RBC and his team have continued to provide facilities which have ensured ongoing success. For the coming year we are looking to insert new members to serve on the chapter executive board because we want to give opportunities to other interested and enthusiastic ACAMS members.

What's next?

The value of having chapters strategically located in a country cannot be understated. The recent expansions in Canada have clearly demonstrated that Canadian ACAMS members want to have opportunities to network and receive ongoing training without having to travel great distances. It is therefore only sensible that we continue to expand our chapter network. Areas that need to be canvassed for the coming year are Calgary and Edmonton, and or one chapter in Alberta. Ottawa is the headquarters of many of our regulators, enforcement agencies and other government institutions, and then pending appetite Saskatchewan, Manitoba and the East Coast. We will be sending a questionnaire out to members in Alberta and Ottawa in the coming weeks to ascertain their desire and willingness to be part of the initial executive.

Having been associated with ACAMS for more than a decade I am proud to continue to work with John Byrne and his team to roll out a vibrant and viable chapter network in Canada. I am a firm believer in T.E.A.M. (Together Everyone Achieves More) and am confident that if we continue to grow with all organizations committing to collaborate we can make a difference in our collective fight against money laundering and terrorist financing.

Conclusion

As a country which has been lauded around the world for the vibrancy and stability of its banking sector, recent events have shown that like many other countries around the world we need to emphasize ethics above greed and ensure the tone at the top also includes our political institutions. 

Garry Clement, CFE, CAMS, AMLP, special advisor; ACAMS, Colborne, Ontario, Canada, gclement@clementadvisorygroup.ca



BUILT FOR YOU.

A NEW INVESTIGATIVE PLATFORM: CLEAR® FOR ENHANCED DUE DILIGENCE

Our customers said they wanted a comprehensive solution that brings all important information on a person or business into one place. They wanted to see associations between individuals and businesses in one view, and understand the risks about a person and their connections. **CLEAR for Enhanced Due Diligence** was built to address the investigative needs of corporate due diligence and corporate security markets. To learn more, go to clear.thomsonreuters.com or call 1-800-262-0602.

Learn about other due diligence solutions for anti-money laundering professionals from Thomson Reuters at accelus.thomsonreuters.com.

Visit clear.thomsonreuters.com
to download our new white paper
on anti-money laundering.

© 2013 Thomson Reuters L-384810/4-13

Thomson Reuters and the Kinesis logo are trademarks of Thomson Reuters.

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



THOMSON REUTERS™

ACAMS RELEASES FINDINGS OF 2013 COMPENSATION SURVEY

Median earnings for CAMS-certified professionals 32 percent higher than non-certified counterparts

The results are in and the findings are clear — AML/financial crime professionals' compensation continues to out-pace general compensation growth. The Association of Certified Anti-Money Laundering Specialists (ACAMS) released the details of its 2013 Compensation Guide on May 15, 2013. With nearly 5,500 respondents, the study is the only one of its kind in the financial crime detection and prevention field. The survey, which groups the data by various criteria, including experience, organization size, and industry, among others, reported a pointed contrast in the earning potential for Certified Anti-Money Laundering Specialist (CAMS) certified professionals, higher median base pay increases for those working in audit and money services businesses (MSBs), and a nearly six percent median overall rate of growth in compliance compensation from 2011 to 2012.

The need for qualified, certified compliance staff rises

Among its most significant findings, the survey revealed that those who had earned the Certified Anti-Money Laundering Specialist (CAMS) credential out-earned their non-certified counterparts by a median of 32 percent, up from 14 percent since the last survey, conducted in 2008. This stark contrast in compensation and growth in the premium for CAMS denotes the high value employers place on the CAMS certification and the desire to have expert staff. ACAMS developed the Certified Anti-Money Laundering Specialist (CAMS) program in 2001 to address the growing need to certify the experience and skills of those tasked with the detection and prevention of money laundering and the combating of terrorist financing. Since its inception, the CAMS credential has proven to be the sought-after designation by employers from both the private and public sectors from around the globe. "I think the survey results clearly highlight the direction and evolution of this field," said John J. Byrne, CAMS, ACAMS executive vice president. "With all-encompassing regulations and more severe penalties and formal

regulatory criticism against not just banks but other financial service providers, the AML community is responding with a greater commitment to hiring and rewarding skilled professionals."

Audit experiences highest salary growth

While the median compensation growth for compliance professionals was nearly 6 percent, certain fields experienced accelerated growth. Those working in AML audit were fortunate to see the highest compensation growth of 8.6 percent. Given recent regulatory criticism for failures in AML audit, it comes as no surprise that employers are willing to pay an extra for those tasked with the audit function. In late 2012, ACAMS developed its first advanced certification — CAMS-Audit. Developed specifically for those who have already earned the CAMS credential, the advanced certification program builds upon that student's expert knowledge and specializes his/her skills to address the audit deficiencies cited time and again by regulators and examiners.

Other significant findings


This year's survey provided several other significant insights. Overall income of professionals in AML and financial crime detection and prevention is up nearly six percent from last year, to a median \$75,500. Salary growth held steady at roughly three percent for most developed countries — including the United States, Canada, and most of Europe — but rapidly developing countries such as India and China led the way with gains of 12 percent and nine percent, respectively.

In conjunction with the full report of the survey, ACAMS members will also receive exclusive access to an online salary calculator based on the criteria collected in the survey. Ted Weissberg, CAMS, CEO of ACAMS, believes that the salary calculator is an invaluable resource for the membership: "The survey results are, of course, insightful and interesting from a high-level overview; however, the most important thing for our members, I believe, is a practical application



that they can use to gauge their own careers." Weissberg explains, "The next step is for members to insert their own personal details to see, on a personal level, what the information means to them."

Byrne concluded, "It is undeniable that the compliance industry and the demand for skilled professionals have skyrocketed. It's a great place to be right now, and we are proud to effectively respond to the changing needs of industry and agency professionals through advanced training, certification and career resources. We are especially committed to equipping the next generation of AML professionals with the necessary tools to jumpstart their careers with a competitive advantage."

The ACAMS 2013 Compensation Survey was conducted by Industry Insights, an independent research firm specializing in association research. The survey was distributed to approximately 60,000 industry employees, ACAMS members and non-members, and received a 9.1 percent response rate. ACAMS members and those who completed the survey will receive full details of the survey; non-members may obtain a copy of the full results by contacting an ACAMS specialist at +1.305.373.0020 or by email at info@acams.org. 

YOUR AD HERE

Don't miss your opportunity to reach a
readership of over 18,000 AML Professionals

TO ADVERTISE HERE

CONTACT ANDREA WINTER:
1.786.871.3030 | AWINTER@ACAMS.ORG

ACAMS Risk Assessment: An in-depth look

This past year has been one of the most truly innovative and customer focused, product development years at ACAMS. In addition to the advanced certification programs, and the expanded regional conferences and seminars across the globe, one of the most exciting new products is without a doubt the ACAMS Risk Assessment tool. As a response to direction received by our advisory board and an organization-wide 2011 survey of our members, this newly developed software is designed to provide a standardized platform for conducting AML risk assessments at institutions worldwide.

Recently, *ACAMS Today* had the opportunity to interview the team at the core of the ACAMS Risk Assessment methodology: John J. Byrne, Esq., CAMS, ACAMS executive vice president, consultants Rick Harms and Ryan Rasske, and Tanya Montoya, ACAMS product development manager. Together they shed some light as to the origins of the project and how it has grown into the comprehensive tool it is today.

ACAMS Today: The ACAMS Risk Assessment tool is a critical endeavor for the AML community. Can you share with us how the project evolved from a simple concept into the comprehensive tool it is today?

John Byrne: Whether you are in the United States or any other jurisdiction, the challenge to the AML professional has always been how to both craft your risk assessment and have some way to determine how your peers are risk ranking. This tool developed by a team of experts does both — provides a detailed methodology for the risk process and a peer comparison component.

AT: In developing the tool, what was the vision behind the risk process and the overall product structure?

JB: The vision at its core is to offer financial institutions worldwide a standardized means of measuring, understanding and explaining their AML risks. To accomplish

this we have responded to the guidance and regulatory requirements of various financial institution supervisors and regulators via a tool that delivers a comprehensive and automated risk profile of an institution's products, services, high-risk geographies and high-risk customer entities.

AT: As the main developer of the ACAMS Risk Assessment tool methodology, can you give us some background on how your work with FinCEN and other organizations have helped you formulate the core features of our product?

Rick Harms: My orientation to a risk-based approach to anti-money laundering work began in the early 80s. I was heading up the U.S. Customs "Artificial Intelligence" system which was one of the first rule-based computerized attempts to identify possible money laundering, based on Bank Secrecy Act data.

We had to employ methods to find "a needle in a haystack." Law enforcement partners in the effort helped us identify specific behaviors and characteristics that resulted in alerts that could evolve into good investigative cases without creating massive numbers of false positives.

This work continued into the first days of the existence of FinCEN when I, the customs unit I headed up, and the rule-based targeting effort all moved under the leadership of FinCEN's first official director, Brian Bruh.

In the early 90s, I carried the same risk-based principles into work that I was hired to do with AUSTRAC. The Australian government had just passed a law that gave AUSTRAC the authority to collect information on all international electronic fund transfers into and out of Australia. I was brought in to coordinate the effort with Australian law enforcement and regulatory partners to develop a risk-based, rule-based system to identify money laundering behaviors amidst the massive amount of international wires.

AT: After your work in Australia, how did you continue to pursue your risk-based concepts?

RH: After Australia followed several valuable years with PWC working on interesting engagements internationally, which led to my being recruited by Rick Small when he was hired by Citigroup to lead their global AML efforts. Rick asked me to work with some great Citi colleagues to develop a standardized AML risk approach to be used globally within Citi. We came up with an objective system that could identify product, customer and geographic money laundering risk. This was truly an exciting and rewarding experience.

In 2008, when Rick Small took over leadership of American Express' global AML organization, he asked me to come apply the concepts we had used at Citi to create a next-generation AML risk assessment system. To my good fortune, my primary partner in this effort was Jim DeRugieriis, whose like-minded thinking had already initiated AML risk work at American Express.

It was really the collaboration with Jim that allowed us to take what I had first started developing in the early 80s at U.S. Customs to the system being implemented today at American Express.

So, when ACAMS approached me to work on your risk assessment tool, my first response was to make sure Rick Small was on board because anything I'd have done would be

This tool provides a detailed methodology for the risk process and a peer comparison component

John J. Byrne, Esq., CAMS



John J. Byrne, CAMS is executive vice president of the Association of Certified Anti-Money Laundering Specialists or ACAMS. ACAMS is the 18,000 member organization that develops anti-money laundering/sanctions/financial crime detection programs and certifies specialists in financial and non-financial businesses and government agencies. The web site is www.acams.org.

Byrne is a nationally known regulatory and legislative attorney with close to 30 years of experience in a vast array of financial services issues, with particular expertise in all aspects of regulatory oversight, policy and management, anti-money laundering (AML), privacy and consumer compliance. He has written over 100 articles on AML, represented the banking industry in this area before 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 Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the ABA's Distinguished Service Award for his career work in the compliance field.

Rick Harms, PhD in Earth Sciences

Rick Harms has a doctorate in Earth Sciences from the UC Berkeley and has 30 years of experience in domestic and international anti-money laundering work. After twelve years as a college professor, Harms began his career in anti-money laundering work in 1983 by joining the U.S. Customs Financial Intelligence Branch. He became the director of that unit, and when the Treasury Department created FinCEN in 1990, he became one of the original assistant directors. From 1992 until 1995, he worked as a consultant with AUSTAC in Sydney, Australia, developing money laundering detection and suspicious transaction reporting systems. In 1995, he returned to FinCEN as a senior advisor, focusing on work with the Egmont Group.

In 1997, he joined PricewaterhouseCoopers, where he directed AML work for gaming, banking, insurance, securities, asset management and corporate clients internationally.

Harms joined Citigroup in December 2001 to enhance the company's AML risk policy, manage the expansion of Citigroup's global AML analysis capabilities, and help implement a unified AML IT strategy.

Since Harms left Citigroup in March 2006, he has consulted on his own with financial institutions, AML service providers, and AML software vendors on a number of projects. He has focused chiefly on AML risk policy and transaction monitoring business rules, as well as the organization, staffing, training, and equipping of FIUs.

Harms' work has focused primarily on American Express' risk policies and monitoring strategy since 2008.

Tanya Montoya



Tanya Montoya has over 15 years in global marketing management and strategic brand development for a wide range of corporations, industries and governmental organizations. Montoya has successfully deployed numerous brand initiatives, both in traditional and online environments.

In her role as product development manager for ACAMS, Montoya is responsible for the development and launch of the association's first Risk Assessment software designed to offer financial institutions worldwide, a standardized means of measuring, understanding and explaining their AML risks.

Montoya has a master's degree in International Affairs from Florida State University, and a bachelor's degree in International Relations from Florida International University.

Ryan Rasske



Ryan Rasske is the founder and president of RiskGap Advisors, LLC. Prior to starting RiskGap Advisors, LLC, Rasske was senior vice president, Risk & Financial Crimes Director for Associated Banc-Corp, a diversified bank holding company with \$22 billion total assets. In this role, Rasske established an enterprise risk management (ERM) framework consisting of risk intelligence

reporting to the board of directors. Additional areas of responsibility included business resumption, anti-money laundering, physical security, internal/external criminal investigations and enterprise-wide fraud.

Before joining Associated, Rasske was employed with the U.S. Secret Service in the Washington D.C. metropolitan area. His banking career started at E*TRADE Bank as the Bank Secrecy Act and Anti-Money Laundering officer and he joined Associated Banc-Corp in 2003.

Rasske currently serves as an advisory board member and faculty for the American Bankers Association (ABA) National Compliance School, Board of Advisors for the ABA Online Professional Compliance Curriculum and Capstone Advisor for the prestigious Stonier School of Banking at Wharton University. He has written several articles for the ABA Bank Compliance magazine and is frequently requested to speak at national conferences such as the *ABA Regulatory Compliance Conference*, *ABA Money Laundering Conference*, and the *NACHA Payments Conference*.

Rasske has a bachelor's degree in Management and Business Administration. He has completed training in Enterprise Risk Management at Kellogg School of Management and holds Stanford University's Strategic and Risk Management Professional Certification.

based on my current American Express work. It turned out that working with ACAMS on such a tool was, in fact, Rick's idea. And so it evolved.

AT: Having had formal experience with both government regulatory agencies and the private financial sector, what do you see as the biggest advantage to financial institutions in using the ACAMS methodology to run their AML risk assessments?

RH: That's a great question and I hope my background and work experience equip me to give you a constructive answer.

My hope is that our ACAMS Risk Assessment methodology provides an alternative for financial institutions that don't have their own resources to meet their growing AML obligations independently.

The biggest advantage financial institutions will discover is the tool's ability to accommodate any size

In addition, I feel that users of our methodology will find the following three advantages.

First, we have taken an objective, repeatable approach that is based on authoritative international sources of information on the money laundering and terrorist-financing risk posed by products/services, customer types and jurisdictions.

Second, we have sought consistency with the published advisories and guidance from the financial regulatory community. Therefore, the regulatory community will hopefully find comfort in and support the underlying premises of our methodology.

The final big advantage for a user is being viewed as employing a robust standardized approach with which the regulators are familiar.

AT: As key contributor to the ACAMS Risk Assessment tool, can you give us a little bit of background on your AML work with E*TRADE,

Associated Banc-Corp, and the ABA, and how that experience has helped you formulate some of the core features of our product?

Ryan Rasske: Each of my experiences were influential and contributed to the design of the ACAMS Risk Assessment tool. My first introduction to risk assessments really came from working for the U.S. Secret Service. This profession provided me with the training and a unique skill-set to mitigate threats by understanding what to look for, calculating the probability of negative outcomes and knowing the proper response.

As I moved out of law enforcement and into banking, I learned these same basic fundamentals could be applied within a corporate environment. In 2001, I became the BSA/AML officer for E*TRADE Bank and began customizing the assessment of electronic banking risk to match the AML complexities of operating in a branchless setting.

In growing my network with AML experts during the turbulent regulatory changes resulting from 9/11, I was introduced to several members of the ABA including John at the time, which turned out to be quite fortuitous. This partnership opened several opportunities to develop best practices, mentor and provide training to others through a variety of channels. Today, I continue to serve in an assortment of roles, including faculty member for the Stonier Graduate School of Banking and ABA National Compliance School.

While at Associated Banc-Corp, I was able to expand my risk knowledge by leading a team to design and implement an enterprise risk management framework. Establishing this type of structure, which included AML risk, promotes the company's ability to analyze risk holistically, aggregate risk types, and develop influential dashboards which provide bank leadership relevant risk scores along with sufficient information to make strategic decisions.

AT: What do you see as the biggest advantage to financial institutions in using the ACAMS methodology to run their AML risk assessments?

RR: It has been a great experience working with ACAMS on this project and truly an honor to work alongside some of the best minds in the AML industry. It's difficult to isolate just one benefit, especially when a tremendous amount of time and energy was applied to the different functionalities the tool offers. With that said, the biggest advantage financial institutions will discover is the

tool's ability to accommodate any size or level of complexity within numerous products or services combined with scoring flexibility and management reports to fit their specific risk profile.

AT: What would you say are the strongest benefits of the ACAMS Risk Assessment tool?

Tanya Montoya: Our software was designed as an answer to the membership's most pressing concerns on evaluating an institution's risk profile, and all product features were tailored to meet those exact needs. There are several benefits that I would define as "strong" and if I could touch on the top four, I would say *total transparency* on how we arrive at our inherent and residual risk scores, *consistency in methodology* across lines of business, access to *peer assessments for benchmarking* and future *standardization* efforts, and certainly one of the most exclusive opportunities our tool offers is access to the *ACAMS community of experts and knowledge center*. ACAMS offers the world's leading AML/CTF certification and education and training, as such, we are in the unique position to be able to offer a continuous flow of information to our users, from timely notifications on new guidelines and enforcement actions that would affect a user's risk assessment, to seamless updates that address any changes in the regulatory environment.

AT: How does the tool take into account weighting and volumes?

TM: The past year has been a year of listening to our members' "must-have" features for the tool — and one of the most repeated requests was the inclusion of a quantitative data analysis to products, customer types and geographies. This would address step two of the FFIEC's BSA/AML Exam Manual requiring a more detailed analysis of the identified data to better assess the risk within these categories. Ryan Rasske, along with the committee of experts was instrumental in making this a reality and we have since implemented a method that allows the user to gain an understanding of each risk factor and to understand the potential impact behind each data point — with the end goal of applying appropriate controls based on the risk profile of the institution.

Furthermore, the gathering of quantitative risk data within our AML risk assessment tool provides objectivity by creating

a risk-based analysis derived from concrete facts which in turn offers a true projection of impact so that management reviews are solution driven sessions rather than verification and validation exercises.

AT: One of the most daunting tasks for a compliance officer is combining automation with documentation when running their risk assessments. How does the ACAMS tool address this need?

JB: As mentioned before, transparency is one of the key elements driving a standardized risk assessment for our users, and clear documentation is certainly part of this process. Within our tool, users have the opportunity to add narratives and document every step in their decision-making process, including control detail, score changes and the uploading of supporting files.

AT: What is the final output after completing the assessment? Does the tool offer graphs and charts?

TM: Yes, our uniquely formulated numerical scoring can be interpreted via numerous presentation ready summaries, reports, charts and heat maps to provide clear communications to both the board and examiners. The tool has the capability of generating detailed reports of inherent and/or residual risks organized by high, medium and low. Reporting includes high level views and executive summaries for lines of businesses, down to a highly granular and detailed report on the institution's controls and its plan of action for risk mitigation.

AT: The question weighing on every compliance officer's mind is the inevitable, what does a tool like this cost and are there additional capital investments needed on site?

JB: As a membership driven AML/CTF organization we truly understand the budget constraints that institutions worldwide face in their daily fight against financial crimes. For this reason, our product was designed as a web-based system requiring no additional hardware installations, or on-premise hardware investments. Consistent with this strategy is also our pricing strategy which is structured against an institution's asset size. **A**

*Interviewed by: ACAMS Today editorial.
For more information about the Risk Assessment tool contact Tanya Montoya at tmontoya@acams.org*

ACAMS® | Risk Assessment

MEASURING, UNDERSTANDING, AND EXPLAINING AML RISK



Standardized Scoring & Reporting



Save Time & Expense Through Comprehensive Automation



Objective Industry Benchmarking

Schedule your LIVE DEMONSTRATION today — contact Tanya Montoya at tmontoya@acams.org or by calling +1 305.530.0913.

ACAMS® | Risk Assessment

The case for centralized KYC

As the cost of addressing new regulations eats away at profit margins and regulators impose record fines, financial institutions (FIs) are actively seeking new solutions to reduce costs whilst raising standards of compliance. For more than a decade, many have consolidated operations into global processing centers. This has driven down costs considerably, but more is needed. Relocating global centers to cheaper locations is not really an option. The next logical step must be shared services.

A clear opportunity exists to leverage a shared service model for the Know-Your-Customer process (KYC). Currently, every FI conducts documentation verification and validation for each client, even when they share clients with other FIs. The same documentation is assessed repeatedly across the industry, often to varying standards.

Centralizing the KYC process and providing a single certification of each client will drive out inefficiency, speed up onboarding, raise levels of due diligence and aid regulators and law enforcement.

The KYC process today

The current KYC process has inherent inefficiencies and weaknesses as detailed below:

Inefficiency: In the current bilateral model, clients provide a similar set of documentation to each FI. Each FI then evaluates that documentation and conducts various background and blacklist checks before accepting the client. The process is then repeated across the industry. This is a significant waste for both FIs and clients who must allocate resources to manage the process across multiple relationships operating on differing timelines. This is then compounded by recertification requirements and expiry of documents.

Slow to Market: The onboarding process can take anywhere from hours to months, depending on the client's ability to provide documentation or how flexible the FI can be in modifying its requirements to accept what the client is able to provide.

Inconsistency: Most regulators do not specify the precise documentation requirements to satisfy KYC due diligence. It is therefore left to the FIs to interpret the requirements; and opinions vary among compliance officers in each jurisdiction.

Conflicting Interests: Whilst KYC specialists are intent on ensuring that due diligence is carried out thoroughly, their performance is assessed on how quickly they can process accounts. Management focus is on getting the account set up as fast as possible to start trading. Depending on the culture of the FI, this can result in accounts being set up before proper due diligence has been completed.

Underinvestment: Regulators have expressed serious concerns about significant underinvestment in KYC functions across the industry. The client onboarding process has historically been underinvested. Even prior to the financial crisis, FIs preferred to invest in the front office, revenue generating staff rather than balancing the need for good quality, well-trained KYC staff. Even now, they prefer to invest in generalist staff rather than invest a little more to ensure that they have highly trained (CAMS certified) specialists. This has created a 'tick-the-box' approach to KYC that often fails to meet the minimum regulatory requirements.

Validation of Documents: Certain jurisdictions require an inspection of original documents by the FI's officers. This is often impractical, especially for a client in an offshore location. One solution to this has been certification by a notary public or other trustworthy source, yet there are major flaws with this approach. How reliable is the notary public or other source's endorsement? Do the FIs check back with the source to ensure that they did in fact certify the documents and are qualified to do so? Whether the validation is performed by the FI's own officers or other source, officers generally lack the equipment and specialist training to identify false or forged documentation. To truly authenticate an ID document, it must be scanned with a specialist scanner and assessed against anti-forgery criteria for that specific document.

Recertification: There is a vast backlog of recertifications at a number of FIs. With resources struggling to keep up with the demands of the volume of new accounts, many FIs are taking a fire-fighting, project approach to recertifications, effectively pushing the problem out for another couple of years, when it will likely resurface again.

Pressures on FIs, and particularly on KYC functions, have created systemic weaknesses that undermine the foundation of the AML framework, leaving the door to the financial system wide open for criminals and terrorists.

Market response

Developments in the infrastructure for KYC currently revolve around the following:

Process Enhancements: FIs and vendors have focused on incremental improvements to the current bi-lateral model. Whilst these improvements have reduced the time required to process documents, they do not address other weaknesses in the system: inefficiency, inconsistency, conflicting interests and document validation.

Data Repositories with Data/Document Exchange: These initiatives are aimed at enhancing the quality of data available to FIs and providing a repository for FIs to access documents when needed. These go a long way toward improving the current process. However, inefficiency remains: the FIs still need to conduct documentation reviews themselves and now rely on electronic copies of documents that have been uploaded by clients, with no reliable validation of those documents. The challenges of inconsistency, conflicting interests and document validation remain.

So the market is making improvements, but is there a more complete solution?

A new model

All of these weaknesses could be addressed by moving to a new model. An independent solution that promotes true efficiency for the market, removes conflict of interest, promotes consistency and significantly improves time to market. A solution for

which KYC is a core competence and which will raise the bar significantly on standards of client due diligence.

Centralized KYC certification

An independent centralized KYC certification platform will address the current systemic weaknesses and inefficiencies, providing the opportunity to significantly raise the standard of client due diligence and closing the doors to the financial system for known criminals, terrorists and their financiers.

Addressing all of the weaknesses in the current system on an institution-by-institution basis would be prohibitively expensive and require an inordinate amount of effort. Creating a centralized solution enables pooling of resources, thus transforming the KYC environment whilst making it significantly cheaper for everybody.

Solving current problems

So how does centralized KYC certification resolve the inefficiencies and weaknesses in the current model?

Efficiency: Clearing client documentation through a single platform would eliminate repetition every time a client opens a new account with another FI. When recertification is required or documents are expiring, the client is approached only once for updated documentation.

For FIs, there is no need for each one to evaluate the documentation for KYC, or conduct background and blacklist checks on the same client. The central platform will perform each

of these tasks once on behalf of all FIs, eliminating duplication across the industry.

Quick to Market: Once the client has been validated by the central platform provider, they would be certified for KYC. When an FI onboards that client, the KYC certification is confirmed as soon as the client authorizes that FI to onboard them.

Consistency: With a clear understanding of multiple FIs' documentation requirements, the KYC platform would be able to determine a universal set of documentation that would enable account opening with any FI in any jurisdiction for any product. Comparing documentation requirements across FIs would highlight inconsistencies that could then be analyzed to determine whether that document is actually required. This would move the industry toward a standardized set of documentation, whilst allowing for differentiation where necessary (e.g., based on requirements of the FI's parent regulator). Some level of customization of requirements would still be needed, hence a universal set of documentation, rather than a standard set.

Avoids Conflicting Interests: The centralized KYC platform would be independently accountable for the completeness and integrity of the KYC certification. This will protect it from compromise by any party trying to circumvent the system to quickly close a lucrative deal.

Appropriate Investment: As a core competence of the platform, the appropriate investment would be made in resourcing and initiatives to ensure the highest standards of KYC are maintained.

Validation of Documents: With suitable investment available, a centralized KYC platform could support specialist training and equipment for officers to accurately assess and validate documentation, readily identifying fraudulent or suspicious documents. This would help remove fake documentation from the market and make a significant contribution to the fight against money laundering.

Recertifications: Recertifications would be a core deliverable of the platform and with appropriate investment in resourcing, the platform would be well positioned to provide ongoing, timely recertification of accounts.

Additional benefits

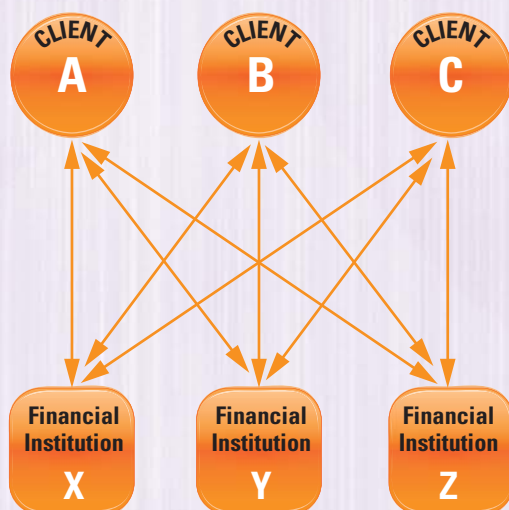
Introducing a centralized KYC platform would result in additional benefits.

Regulatory Efficiencies: With a single centralized platform to audit for KYC, regulators around the world would be able to save significant resources whilst ensuring the quality and integrity of the process performed by the central platform.

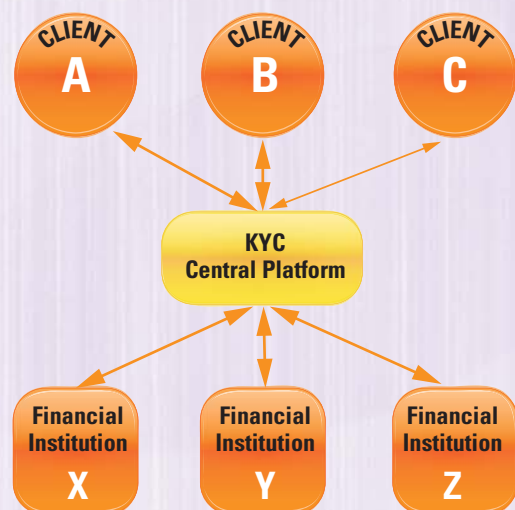
Support For Law Enforcement Agencies: A tighter KYC regime would force criminals to further remove themselves from any accounts being used for financial crimes. This would extend the chain of individuals involved, giving law enforcement more opportunities to intercede and break the chain.

Static Data Upload: During the document verification process, static data could be scrubbed directly from the documents. This

Current Model



Proposed Model



could then be downloaded by FIs to facilitate the automation of account setup across multiple systems.

Single Legal Entity Identifier: By default, a centralized KYC platform would generate a single legal entity identifier (LEI). The platform could work with FIs to automatically generate their client codes. The platform would maintain mapping tables of client accounts for each FI. The LEI would be maintained centrally on the KYC platform and easily mapped to the relevant accounts at each FI.

Making it happen

To make centralized KYC a reality, several key components will need to be put in place to address common concerns with this model.

Regulatory Approval/Acceptance: Whilst current regulations in many jurisdictions allow for outsourcing of KYC, the concept of a centralized certification of KYC for re-use has not been specifically addressed.

The industry will need regulators to confirm their acceptance of this model before it can be fully developed and implemented.

Global Coverage, Local Support: In order to avoid fragmentation of FIs' processes, the centralized KYC platform would ideally provide global clearance for each client. FIs — especially those that have already centralized their processes internally — would want to go to one platform and see the client cleared globally. They do not want to use different methods for clearing accounts to trade in different jurisdictions.

The platform would also require multi-lingual systems and support to facilitate operations in local markets — especially in Asia.

System and Data Security: System and data security are probably the most important concerns of a centralized model.

The system would need to be designed with best in class, state-of-the-art security, at least on par with that of banks, exchanges and governments today.

Key elements that would need to be addressed would be: physical security of hardware; system architecture design; and user authentication and authorization methods.

Data Privacy: The platform would need to comply with data privacy regulations of various jurisdictions, particularly with regard to maintaining client data onshore

and ensuring client permission is obtained to use the data for each different purpose (i.e., when providing KYC certification to each FI).

Meeting the requirements for onshore storage of data could be as simple as maintaining data on an onshore server. Where regulators insist on the operation itself being onshore, FIs will already have onshore resources allocated to KYC. Consolidating those resources into a local KYC platform would still make sense.

To address concerns about client data being used for a purpose other than that for which it was gathered, clients would be required to approve use of their information by any FI before the KYC process is initiated.

Liability for failures of KYC: In order for this approach to work fully, responsibility for KYC certification of a client must lie with the centralized KYC platform. Responsibility for failures in the KYC process, whether fraudulent, negligent or accidental, would have to remain with the platform and not transfer to the FIs.

Each FI will own the relationship and the decision as to whether to adopt the client or not.

An agreement will be needed from the regulators that if an FI establishes a relationship and transacts with a client erroneously cleared for KYC, and where the FI(s) would have no other indication that the client is unsuitable, then the platform provider, not the FI(s) would be held liable for any injury or damages resulting from that relationship.

Simple transition and interconnectivity for each FI: Transitioning FIs onto the KYC platform could be as simple as having onboarding officers manually check the KYC status on the platform. Or it could be as sophisticated as establishing connectivity with client onboarding systems to integrate the KYC platform into the FI's process flows.

Asia first?

Given the challenges of building a global platform, a phased development approach would be needed. In order to be a truly global solution, the platform would need to handle requirements of varying degrees of sophistication across multiple jurisdictions. Developing the initial platform in that environment would ensure that the foundations are laid to support the high levels of complexity that will arise as new jurisdictions are added.

Asia is perhaps the best place to start building this global platform.

Asia is effectively more than 30 regions in one, with many different approaches to KYC and AML requirements. Whilst some of these jurisdictions have collaborated to work toward more consistent standards, and a centralized approach might encourage others to follow suit, this will take time and not all would do so. Asia thus provides the level of sophistication needed to challenge the foundational design of the platform and ensure that it will work as a global solution.

Regional regulators, whilst fully understanding the cost and client acquisition pressures on FIs, also have a strong and evolving focus on AML. They are taking proactive steps to strengthen the market against criminal and regulatory risk, leading the way in controlling their borders as Asia has grown in significance as a leading global financial center. Both Thailand and the Philippines have updated their AML Acts this year, increasing the powers of AML authorities and expanding a number of related definitions, including predicate offenses amongst others.

Asia is also traditionally the home of smart-sourcing and utility services. Originally this was a wage arbitrage but now there is a pool of experts that have been looking at KYC/AML for almost a decade.

Once the concept has been developed and proven in Asia, it could easily be rolled out globally by adding new jurisdictions to the platform with appropriate language and time zone support.

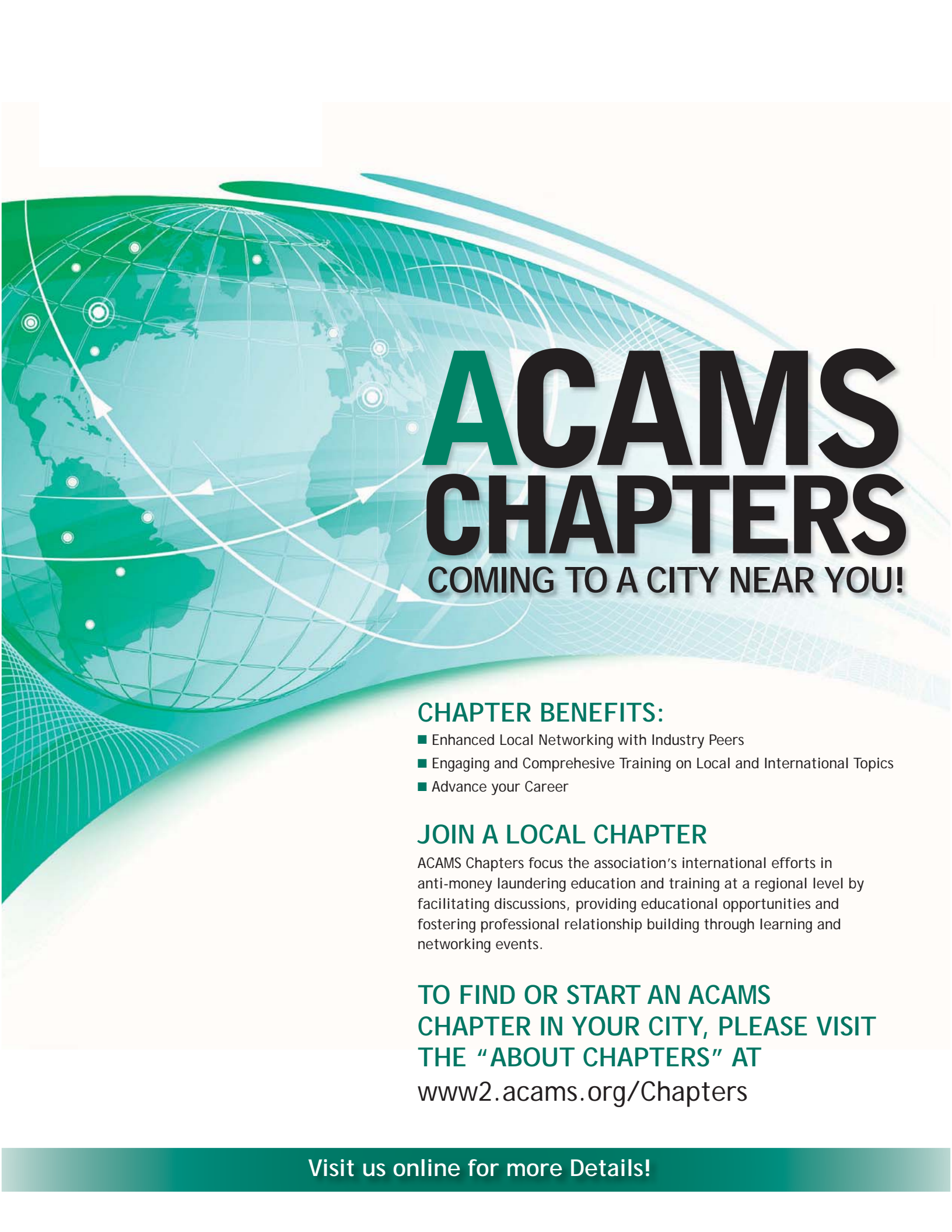
Conclusion

An independent centralized KYC certification process is a compelling solution to many of the systemic weaknesses and inefficiencies inherent in the current model. It would also provide a platform to significantly raise the standard of client due diligence and help close the doors of the financial system to known criminals, terrorists and their financiers.

All the components to build a long-term solution exist today. With support from the regulatory community, the engagement of several leading FIs and the use of available technology, it is possible to build a truly transformational centralized KYC platform today. **A**

Bryan Shillabeer, partner, TBD Solutions Pte Ltd, Singapore, bryanshillabeer@tbds.biz

Derek Venn, partner, TBD Solutions Pte Ltd, Singapore, derekvenn@tbds.biz



ACAMS CHAPTERS

COMING TO A CITY NEAR YOU!

CHAPTER BENEFITS:

- Enhanced Local Networking with Industry Peers
- Engaging and Comprehensive Training on Local and International Topics
- Advance your Career

JOIN A LOCAL CHAPTER

ACAMS Chapters focus the association's international efforts in anti-money laundering education and training at a regional level by facilitating discussions, providing educational opportunities and fostering professional relationship building through learning and networking events.

TO FIND OR START AN ACAMS
CHAPTER IN YOUR CITY, PLEASE VISIT
THE "ABOUT CHAPTERS" AT
www2.acams.org/Chapters

Visit us online for more Details!

Ted Weissberg, CAMS Chief Executive Officer



A *CAMS Today* spoke with Ted Weissberg, CEO of ACAMS to get his thoughts on training, ACAMS and other matters.

Prior to joining ACAMS in 2009, Weissberg was president of the Information and Training unit of Fortent, Inc. and spent 15 years at Thomson Financial in various editorial, publishing and general management roles, including president of Thomson's Venture Economics unit. In total, Weissberg has worked in the information and training field for more than 25 years. Weissberg is a graduate of Wesleyan University. He has authored two books, a biography of Arthur Ashe, and an exposé of NCAA sports scandals.

ACAMS Today: How did you first become interested in the financial crime field?

Ted Weissberg: I started working in the field in the end of 2005. I knew very little about financial crime before then, but I quickly became fascinated by it.

AT: What has surprised you most about working in the compliance industry?

TW: The level of cooperation and camaraderie among people in the industry. I had never seen so much collaboration among professionals at competing organizations. It quickly became clear to me that the people in this industry feel deeply that they are doing important work, both for their employers and for our society as a whole, and that they are perfectly happy to share

their practices and strategies with peers, knowing that they may learn something valuable in the give and take.

AT: As CEO of ACAMS, what do you hope to accomplish in the next couple of years?

TW: I am very happy with the course ACAMS is on and I want to continue that and see through the initiatives we're working on today. For example, I want ACAMS to continue to globalize, and I expect in a couple of years' time about half of our membership will reside outside of the U.S. I also want to encourage the continued rapid growth of membership. We're up around 18,000 now, which is about double where we were three years ago. And I want to continue to introduce new training programs, conferences, certifications and other tools to meet the emerging needs of the industry.

AT: When you attend ACAMS' conferences around the world, what is the most common theme you hear discussed amongst the compliance professionals?

TW: Perhaps the most enduring theme, regardless of the regulatory demands of the day or the region, is the sense that the jobs of our members are becoming more difficult and bigger all the time, and that the stakes keep getting higher.

AT: What is one of your favorite products that ACAMS offers?

TW: It's hard to choose just one; we love all our children. The CAMS certification program is at the core of what we do and has played an important role in professionalizing the industry. I'm very proud to be

a part of that. I am also very excited about ACAMS Risk Assessment, a tool that we will be launching in the fall to help financial institutions conduct their AML risk assessments more easily and according to an industry standard. The first product that I was involved with was a predecessor to Money-laundering.com, so I have a soft spot in my heart for that excellent information resource. And, of course, *ACAMS Today*!

AT: In your 25 years of experience in the information and training field, what is the key to building a successful training program?

TW: Getting smart, experienced professionals to tell you what they need, listening closely, asking good questions, and then doing your best to meet those needs — and then adapting the program often and thoughtfully. I also have found that teaching through case studies, whenever possible, is both engaging and effective.

AT: You have authored two books in the sports field. Are you planning on writing another book and if so will it be in the sports genre?

TW: I think my days of book writing are past. I'm too busy. But if I were to take it up again, I wouldn't write another sports book. Maybe I'd try a crime novel instead... with an AML compliance officer hero, of course. Detailed descriptions of KYC processes and transaction monitoring policies always sell books, right? **TA**

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

ACAMSToday.org is now mobile!

www2.acams.org/TheApp



ACAMS members may now download the *ACAMS Today App* and read relevant articles and content directly from their mobile devices.

Download the App for:

- Full access to the complete compendium of articles, interviews, polls and exclusive content available to ACAMS members
- An easy-to-use interface that allows you to find the information important to you
- Convenient access to content wherever and whenever you want

Get the app now at
www2.acams.org/TheApp



ANALYTICS

Catch money launderers in the act.

SAS® Anti-Money Laundering delivers dynamic risk assessment that classifies relationships as low, medium or high risk, so you investigate only meaningful alerts. Decide with confidence.



sas.com/alert
for a free white paper


THE POWER TO KNOW®