

ACAMS[®]TODAY

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

Women in AML: A beacon to the community 38



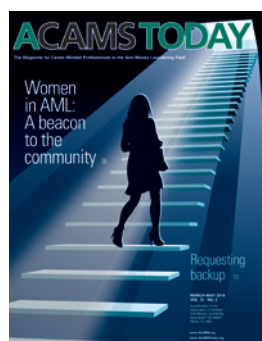
Requesting backup 70

**MARCH–MAY 2014
VOL. 13 NO. 2**

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

www.ACAMS.org
www.ACAMSToday.org

ON THE COVER



Women in AML:
A beacon to the
community
38

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

Editorial Assistant

Alexa Serrano

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

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

Principal, Ernst & Young, LLP,
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 of AML
Compliance, Financial Crime
Risk Operations, HSBC
Holdings Plc, 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

Anna M. Rentschler, CAMS

Vice President & BSA Officer,
Central Banccompany,
Jefferson City, MO, USA

**Anthony Luis Rodriguez,
CAMS, CPA**

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

Nancy Saur, CAMS, FICA

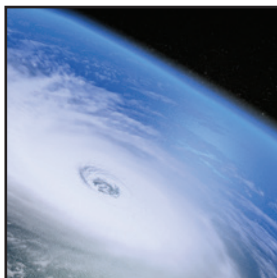
Head of Compliance,
Advantage International
Management (Cayman) Ltd.,
Cayman Islands

Markus E. Schulz

Chief Compliance Officer
GE Capital International,
London, UK

Daniel Soto, CAMS

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



- 4** From the editor
- 4** CAMS and Advanced Certification Graduates
- 8** Member Spotlights
- 9** A message from the executive vice president
- 10** Leaving a legacy with CAMS-Audit
- 12** Intermediary funds transfers: The eye of the AML storm
- 18** From smurfs to mules: 21st century money laundering
- 22** Assessing the convergence between terrorist groups and transnational criminal organizations
- 26** A "C" change for virtual currency
- 30** Regulators 'doubling down' on their scrutiny of casinos
- 32** FATF takes aim at 7 'Hawala Myths'
- 38** Women in AML: A beacon to the community
- 39** Nancy Saur, CAMS: The energizing field of AML
- 42** How can you not?
- 44** Suzanne Williams: Never stop learning
- 46** HE Ying: The importance of knowledge and practice
- 48** You can play a critical role in our nation's national security
- 50** "Connecting the dots"
- 54** Barbara Keller, CAMS: AML—the mansion industry
- 56** A modern day heroine and her fight against human trafficking
- 58** Women in AML showcase
- 68** The why and how of writing a no-SAR justification
- 70** Requesting backup
- 72** A new approach to adverse media for enhanced due diligence
- 76** AML Systems: Planning for successful implementation
- 80** Goldilocks and the three sanctions
- 82** Singapore—picks up the pace in combating economic crime
- 86** Interview with Chief Commissioner of MACC
- 90** Meet the ACAMS Staff



On March 8, 2014 we will celebrate International Women's Day. There have been various women that have impacted me in a positive way, in both my personal and professional life. There are too many to list them all by name, but these women have helped in constructively shaping the person that I am today and also in mentoring me in the professional world. Suffice it to say that the impact of women is felt by everyone. The first woman to impact my life was my mother. Later in life it was one of my favorite teachers and then it was my track coach. When I entered into the professional world I had the opportunity to call a few distinguished women my mentors.

The AML world is filled with women who have made an impact both in and outside the AML and financial crime prevention fields. As I worked on putting this edition of *ACAMS Today* together I was fortunate enough to communicate with each of the wonderful women highlighted in the *Women in AML: A beacon to the community* and in the *Women in AML Showcase* either through an interview or an article about their work. The women I spoke with left me with a positive feeling and a sense of pride for receiving the opportunity to interact and work with some of the most distinguished and important women in the AML community. I hope you enjoy the *Women in AML* special section and also the *Women in AML Showcase*. *ACAMS Today* acknowledges that there are thousands of women who contribute to the AML field that we were unable to highlight, but we would like to personally thank everyone who contributes to the daily fight against financial crime.

The *Women in AML: A beacon to the community* section also contains profound articles in the fight against human trafficking. "Connecting the dots" gives us insight on what the community is doing to fight human trafficking and also shares with us the thought provoking statement, "No one can do everything, but everyone can do something" to help stop this horrific crime.

In addition, the women's section contains in-depth interviews with Nancy Saur, ACAMS advisory board member, Suzanne Williams of the Federal Reserve, Barbara Keller who recently retired from Federal service and HE Ying, who is the vice president of Shanghai Finance University.


This edition contains other exciting articles. The second headline article *Requesting backup* discusses the importance of communication between the financial institution and law enforcement during AML investigations and what both parties can do to improve knowledge sharing.

A "C" change for virtual currency touches on FinCEN's guidance and requirements, the different types of virtual currencies that exist and how the media has affected the public's perspective of virtual currencies.

From smurfs to mules: 21 century money laundering takes the reader through the smurfing process and then onto the more sophisticated process of cyber-crime mules. Learn how to identify the red flags in both these scams and how your institution can protect itself.

This edition of *ACAMS Today* is the largest to date and contains many interesting and insightful articles for ACAMS members. Be sure to explore the edition from cover to cover and we look forward to receiving your comments. As always, please send your comments, suggestions and topic ideas to editor@acams.org.

I would like to encourage everyone to take a moment to remember and thank a woman who has impacted your life in a positive way on March 8, 2014, International Women's Day.

Thank you to all the women and men who are constantly fighting against financial crime! 

Karla Monterrosa-Yancey, CAMS
editor-in-chief



CAMS Audit Graduates

ANTIGUA AND BARBUDA

Kem Warner

BAHAMAS

Cherise Cox-Nottage

Yolanda Hilton

BRITISH VIRGIN ISLANDS

Garvin De Jonge

CAYMAN ISLANDS

Lisa Martine Bowyer

Angela Mele

MAURITIUS

Mahendrasingh Ramdhary

NETHERLANDS

Dave Dekkers

SAINT KITTS AND NEVIS

Idris Fidela Clarke

Vincia Herbert

UNITED STATES

Maleka Ali

Joyce Broome

Alicia Cortez

Donna Davidek

Jonathan Estreich

Katya Hirose

Ryan Hodge

Jeffrey H. Houde

Tara R. Johnston

Laurie Kelly

Alba Kiihl

Nancy Lake

Victoria Landon

Sherron Lewis

J. Scott Mauro

James I. Park

Iris Pinedo

Marianne Schmitt

Kenneth Simmons

Brian W. Vitale

Hao Wang



CAMS Graduates: November–January

ANTIGUA AND BARBUDA

Airon Yavé Pino Morales
Kay Simon
Seymore Smith

ARGENTINA

Flor Vidal Dominguez
Juan Pablo Juárez
Martin Kopacz

ARUBA

Cyrielle de Nobrega
Jonathan P.A. Looman

AUSTRALIA

Steven Donald Bannerman
Carlos Bibawi
Joshua McLellan
Anthony Morgan
Ashley Walters

AUSTRIA

Yelena Martino

BAHAMAS

Israel Borba
Alicia Stuart

BAHRAIN

Lulwa Isa Abdulla Al Musalam
Ahmed Hussain Al Radhi
Mohammed Sameer Al Wassan
Sumit Dhadda
Guru Prasad Kanthoor
Pankaj Kherajani
Satheesha Rudrappa

BARBADOS

Tya Marville

BELIZE

Carlos Witz

BERMUDA

Candace Roach

BRAZIL

Jefferson Machado Silva
Ronald Rosado

BRITISH VIRGIN ISLANDS

Delia Jon Baptiste

CANADA

Agil Agil
Julie Bellemare
Paul Burak
Anthony Catenacci
Joshua Cayer
Hai-Yui Cora Chan
Debbie Charles
Anicio Difonzo
Caroline Dugas
Jane Eom
Lili Fan
Gustavo Enrique Fernandez

Marilyn Galloway

Stephanie Gomes

Dennis Gregoris

Lanna Guillen

Archana Hooja

Marshall Hopkins

Sandeep Jayakar

Ellen Johnson

Alison Keilty

Gabriel Kojima

Alice Lachapelle

Sean K. Leahy

James C. Lee

Maxim Legkodimov

Diane Lyall

Judy Merritt

Mayank Mittal

Lydia Nissan

Gina Olarte

John Pierre Ottley

Judaline L. Pereira

Roshan Persad

Marc Proulx

Romesh Rajaratnam

Supreet Rehal

Melanie Rousseau

Andreu Salvà

Geri Savova

Jaclyn M. Sheppard

Rodney Shields

Fraz Siddiqi

Peter J. Sliwinski

Shannon K. Smith

Edward Solino

Zied Naceur Souidene

Peter Taylor

Susan Janet Tippet

Meredith Miller Voliva

Owen Warner

David Washer

Vivien Wong

Chung Man Mandy Yeung

Hyung Min Yi

Eylon Zemer

CAYMAN ISLANDS

Jennifer McKinney

Natalee McLean

Barbara J. Oostervyk

Chris Michael Orlandini

CHILE

Natalia Ivana Manríquez Salinas

Felipe Alejandro Vega Cuevas

CHINA

Qing Chen

Jianfeng Hu

Yue Hu

Guoyun Luo

Qiqing Mao

Kai Min

Xiao Li (Sally) Ou

Fu (Silver) Qinyun

Lijing Shen

Huiqin Song

Yijia Wang

Hailin Wang

Joyce Wing Sze Wong

Keping Xu

Wei Zhen Yu

Jinping Yuan

Minjie Zeng

Jian Zheng

Zhengguo Zhou

Shuibiao Zhou

Shihao Zhou

Qianting Zhu

COLOMBIA

Andrea Diaz Albelaez

Liliana Patricia Donado Sierra

CONGO

R. Sylvie-Marianne Nsimire

CURACAO

Sita Finessi-Kimatrai

Irving N.M. Janga

Astrid Richardson

CYPRUS

Jacqueline Lamberts

CZECH REPUBLIC

Vit Sindelar

Gabriela Tvrdíková

EGYPT

Amr El Bably

FRANCE

Sebastien Daligny

GAMBIA

Ansumana Cham

GERMANY

Alexander Bogensperger

GHANA

Opeolu Anthony Ibikunle

Joseph K. Amoah-Awuah

Adinan Chigabatia

Philip Q. Danso

Henrietta Esi Hagan

Emmanuel Nikoi

Lucy Naa Offeibea Abebese

Acheampong Opoku

HONDURAS

Rennie Raquel Valladares Alcerro

HONG KONG

Marlyne Bidos

Kam Chan

Sara Tsz Wah Chan

Chin Fung Chow

Ryan Kam

Benedict David Brownie Kent

Joseph Wing Fai Lee

Mathew Daniel Elliot Leeks

Joann Leung

Paul Li

Jaime Oh

Chi Kuen Cecily Sing

Jessie Dak Kay Tam

Danna Tang

Huy Gien Andrew Tjang

Chi Man Joyce Wong

INDIA

Robby Abraham

Shalini Chhutani

Pansy D'Souza

Viji Krishnan

Shiva Kumar

Avni Mehta

Rajish Mithra R.

Bhaswati Mitra

Raghavendran Nagendran

Ritin Prakash

Amol H. Raichura

Christy Rajan

Rajalakshmi Ramaswamy

Lakshman Rao Sadhanala

Narendra Singh

Devi Subramanian

Joseph Sumanth

Mukundan T.K.S.

INDONESIA

Mohamad Thayeb

IRELAND

Sinead Burke

Rachel Curtis

ITALY

Tingting Chen

JAMAICA

Kadeisha Bryan-Mitchell

Lisa-Gay Taylor

JAPAN

Chika Ikeda

Hirohisa Katou

Yuichi Kobayashi

Takanori Matsumoto

Kazuaki Miyake

Shunsuke Mizokawa

Hitomi Okada

Hirofumi Suzuki

Junji Takei

Yurika Yajima

JORDAN

Mohammad Al Amayreh

Máen Bashir Al Zoubi

Ayman Al-Malahmeh

Ehab Al-Shalabi

Omar Musa Ballouta

Tamer Wasef Barakat

Nisreen Basbous

Mahmud Mahammad Jamil Hanbali

Lubna Madanat

Hussam Abdulrazaq Mahmood

Anas Nairoukh

Mohammad Amer Abu Rahmeh

Ahmad Saleh

Noor Kanan Touran

Hassan Zebdeh

Eman Zou'bi

KAZAKHSTAN

Timur Borenshtein

KENYA

Michael Mbwavi Lusinde

KUWAIT

Wael Abbas

Abdulrahman Al-Ebrahim

LEBANON

Joseph Elie Armaos

Adib Fayed Barakat

Dania Dorra

Maha Rafic El Khayat

Zeina Ismat Kawass

Paula Salim Khoury

Abdul Hafiz Mansour

Abboud Georges Meaiki

Charbel Moukarzel

Nathalie Habib Nassif

Sawsan Daher Shamsuddin

Mohamad Hussein Zogheib

LITHUANIA

Marius Kuprys

LUXEMBOURG

Aurore Balbastre

Marie Dominique Gordon

Hema Ramsokh Jewootah

Guilhem R. Ros

Christoph H. Winnefeld

MACAU

Im U. Chan

Man Teng Chu

ZhaoSheng Guo

Chi Chio Iao

Wing Yan Gloria Lee

Fei Sut Lei

Jun Lei

Angela Leung

Veronica Renata Pereira Ho

Li Qin

I Mui Tam

Meng Yuan

MACEDONIA

Ilina Garevska

MALAYSIA

WaiFang Chong

Salina Mohd. Hanifah

Eileen Lee

Rajeev Mahajan

Aidan Moriarty

Hee Teck Eric Ng

Gan Haun Sin

Belinda Teh

Yan May (Nicole) Yu

MAURITIUS

Suraj Kumar Parmahans Nosib

MEXICO

Diana Carolina Hernandez Gomez

Ricardo Lechuga Reyes

Daniel A. O. de Montellano Velazquez

Benjamin Serra Cruz

MOROCCO

Omar Benkirane

NETHERLANDS

Rinaldo Mohunlol

Luis Enrique Palomino Ney

Fabian Sanglier

Richard Van Zanen

NEW ZEALAND

Olga Yurevna Mayes

Michelle Eileen Theron

NIGERIA

Stephen Abiona

Olanrewaju Balogun

Cordelia Ifeanyichukwu Denen

Isioma Echiemunor

Okechukwu Ethelbert Iwunz

Obinna Sylvester Okafor

Abayomi Francis Okeowo

Ademilola Oluwabukayo Olafusi

Kayode Temitope Olanrewaju

Olabode Olusola

Victor Oni

Ayobami Akinbode Raji

Nasir Abubakar Song

Joy Ifeyinwa Sulucainan

OMAN

Roy Koodali

PAKISTAN

Durfishan Ainy

Muhammad Jibran Farid

Nabil Juda

PALESTINE

Zaher A. Hammouz

PANAMA

Anna Valdes

PERU

Renato Raffo Regis

PHILIPPINES

Gerard Duran Roura

POLAND

Szymon Blachuta

Krzysztof Kucz

Malgorzata Pilczuk

Eugene Vashkelevich

PUERTO RICO

Denisse Aracena Garcia

Sandra Cecilia Giraldo Giraldo

Omayra Matias

Ada Liz Ramirez

Sahily Nair Rivas Oliveras

QATAR

Devinder Chand

Amro Mahmoud Reda El Demirdash

Muhammad Sarfaraaz

ROMANIA

Similea Elena

RUSSIA

Anastasia Allenson

Alexander Popov

Richard Smith, II

Oksana Yazykova

SAUDI ARABIA

Hussain A. Al Owa

Thamer Hussain Alenzi

Wael Al-Rasheed

Luai Mukhtar

SINGAPORE

David Alexander

Ridhima Gulati

Rui Jie Terence Ho

Mojca Ivezic

Ee Ling Kok

Atul Kundra

Kit Wai Lau

Chooi Hur Lee

Jayagopal Nandagopal

Daniel Cheewai Ow

Wei (Lolly) Wang

Nizam Bin Zaini

SOUTH AFRICA

Jeanetha Brink

Johan Hetzel

Greg Ulyate

SPAIN

Josep Castro Alcantara

SWEDEN

Karl-Johan Karlsson

TAIWAN

Yu-Han Lai

TRINIDAD AND TOBAGO

Raquel D'Andrade

TURKEY

Leyla Caliskan

Ozlem Yakupoglu

UNITED ARAB EMIRATES

Rashmi Agarwal

Hani Ibrahim Ahmad Al Aiwat

Noora Jassim Al Redha

Jyotirmaya Behera

Jeetendra Ganeshlal Bhatia Udeshi

Sarah Currey

Suryaprabha Easwar

Sara Galadari

Sara Haydar Ahmed

Imad Ismail

Wasim Jabr

Morayo Jimba-Falodun

Dhanusha Sunil Kumar

Faisal O. Rifai

Ramnath Sankaran

Anwar Shareef

UNITED KINGDOM

Bukola Adisa

Hayley Braude

Jamie Broom

Heather Buxton

Luis Manuel Canelon

Lewis Claydon

Conrad Critchley

James Diggins

Pascal P. Dirickx

Paul Edwards

Ben Evernden

Samantha Garrett

Fiona Gray

Tom Hill

Stephanie Holmes

Daniel King

Francisco Mainez-Vidal

Isack Moshy

Christopher P. Murray

Samuel D. North

Okechukwu Donald Onwujiwe

Arjun Sahadeva Premkumar

Thomas Preston

Bilal Rasul

Mohammed Aleem Rathor

Svetlana Rhodes

Jaroslav Rys

Lindsay Karen Scholtz

Farrall Scott

Subrina Shakir

Michael Smith

James Thiga

Madga Wrobel

UNITED STATES

George Abinader

Paul R. Achman

David Agresto

Gina Aguirre Jimenez

Korede Michael Akeju

Ahmad Al Hajjeh

Lisa Ali

Jacqueline Marie Allen

Eric Marc Allmendinger

Edward D. Altabet

Carol Amesquita

Michael Amo

Jennifer Anderson

Gayle Andress

Kelly Ansel

Brooke Arden

Benjamin C. Armstrong

Denise I. Arntson

Naiomy Arrington

Marie Artus

Sabrina M. Ashleydale

Andrea Auguste

Jennifer Avila

Jessica Baglo

Balaji Balasubramanian

Buijanna Banda

John T. Bandler

Amy Bargas

Nincy Barroso

Debra A. Bartolerio

Kerri L. Bashore

Paul L. Baxley

Jessica C. Bellanca

Kathleen M. Berigan

Julia Berman

Sanjay Bhatt

Ashutosh Sharad Bhide

Jennifer Lynn Black

Dana Blaylock

Ezra Blumenthal

David Lawrence Bohm

Brian Bonilla

Cariña Booyens

Tracy Boucher

James T. Boudreau

Andrew L. Bovaird

Malcolm D. Boyd

Amalia Bracho

Amy L. Britton

Rachel N. Brown

Steven Brown

Kimberly Brown

Ralph O. Brune

Anna M. Buck

Christine Lynn Bucy

Nicole M. Budica

Keith Bui

Christi Burge

Meghan C. Burns

Michael J. Bussi

Miguel Angel Bustamante

Antonio Cabiness

Angelita V. Cabrera

Janira Calahan

Luis S. Campos

Li Cao

Brad Carroll

Peter Causey

Brian Chan

Marilyn Charlot

Natalie Simone Chin

Amy Cho

Mandy Man Lok Chow

Lisa Christensen

Megan Christianson

Crystal Chu

Joseph M. Ciccolo

Christine Alexandra Cioffi

Benjamin Ciurdar

Rachel Clarkson

Mark Coalter

Stephen G. Coburn, Jr.

Monique Codjoe

John Concannon

Daniel R. Cordero

Cindy A. Corrica

Dennis Coy

Philip N. Crawford

Kristine R. Curl

Paula Curry

Lisa D'Alton

Stephanie Daniel

Matthew Dankner

Michael Davis

Kirby Davis

Jessie J. Dean

Cheryl Ann DeHaut

Paul A. DeSanctis

Brad Dethloff

Grace Dibi

Matthew Dietrich

Maria Victoria Dolor

Alina Doran

Gene Doucette

James Driver

Nicolas Dubon

Craig Edwards

Ana Mary Egan

Steven Eisenhauer

Daniel Elder

Mark Kerr Elliott

Erin Nicole Elliott

Angela Ellis

Jonas Emilsson

Kevin R. Erdman

Rebecca L. Escario

Yuan Fang

Jie Fang

Kevin E. Farrell

Ashley Farrer

Luis Javier Fernandez

Sydney E. Fetter

Robert Filteau

Ashley Fink

Emily Fischerkeller

Jonathan Xavier Flagg

Holly Flowers

Timothy Flynn

Allison Flynn

Meghann R. Fogarty

Greg M. Forgang

Sue Fouts

Joseph Franzzone

Marshall A. Freund

Jennifer A. Galvez

Obed Garcia

Hillary Gardner

Thomas M. Garry

Edna Carolina Garzon

Kelly Geffert

Krista A. Gensler

Matt Genzink

Joseph Gibson

Joseph Geebor Gibson Jr.

Miriam Gil

Andrew W. Goering

Brian Golden

Lourdes Gonzalez

Brian Alexander Gordon

Mavis Gragg

Alexis D. Gray

Jill Green

Amy G. Greene

Svetlana Grey
Carla Grice
Branton Grimes
Judith Grivich
Daronn Grosvenor
Nicholas A. Gruber
Elissa B. Gruber
Richard Guerci
Matthew Guggenheim
Christopher Gumm
Chris Haller
Afsheen Hamdani
Joseph W. Hammon
Sharif Rasul Hannan
Debra L. Hansen
Taryn Harris
Randy Johnathan Harris
Farid Hashemi
Joseph William Hayes
Stefanie Heichel
Ariel Carlos Helfenstein
Benjamin Henkes
Jessica L. Herbert
Alberto Hernandez
Ignacio Javier Hiraldo
Kate Hirschhorn
Deb Hoff
Bryan Holder
James Holding
Steven T. Holly
Teresa Howard
Joanie Hsu
Chia-Jung Hsu
Kristi Hsu
Danyan Huang
Vivian Hwang
Sandy N. Jabado
Petr Jelinek
Kelly M. Johnson
Brent Johnson
Rachelle Johnson
Robert Jordan
Elliott Jorge
Rebecca Joseph
Robert J. Kaehler
Timothy Kali
Michael M. Kaneshiro
Ehren Kappe
David Katz
Jonathan Emile Kay
Sue Kessen
Richard Kim
Sean Kinard
Seth Kinley
Shervalee Knoll
Lynn Koberstein
Yelena Kobzar
Rebecca C. Koh
Abhishek Kohli
Tara Gerhold Kokollo
Ben Kolb
Paul A. Kramer
Jessica Alyse Kremer
Peter J. Krusing
Dawn Krutz

Matthew Kuhl
Sarvesh Kumar
Nitu R. Kumar
Indrajeet Kumar
Subramanyam Kurapathi
Karin Lam
Kenneth Lam
Sarah Larson
Patricia M. Lasater
Aldo Lau
John LaVerghetta
Candace Lawson McLawrence
Angela Lee
Sunny Lee
Marcia LeFleur
Christopher Lega
Kaitlin H. Lemmo
Linda Ann Leo
Karen Leonard
Rick Leong
Joseph Leva
Avraham A. Levitan
Tanya Levsen
Yi-Hsiang Liao
Patrick D. Lightcap
Eveline Irene Lingenfelter
Ken List
Douglas Litowitz
Laura Louzader
Andrew Michael Lubow
Daniel B. Lundstrom
Matthew Phillip Lupo
Joseph Maida IV
Jerona Maiyo
Mike Makula
Barbara Mallon
Mahabir Mangra
Ameya Ramesh Marathe
Audrey M. Marcum
Jim Marek
John Marinella
Alex Marroquin
Brock Marshall
Barbara Ilene Matthews
M. Tate McAuliffe
Franklin McCrary
Judy A. McGinnis
Taylor McIntire
Michael Edward McLaughlin
Todd McPeak
Jose Medina
Jose C. Medinanazer
Timothy W. Meehan
Arlene N. Mejias
Enrique C. Melencio
Arnold Mendelsohn
Mark Mendes
Miguel Mercado
Sarah Meyer
Samantha Meyers
Kathryn Miller
Idalia Miranda
Hussain Mirza
Judy Mitchell
Nicholas J. Mitchell

Julianne Mixtacki
Abdul-Malik Mohammed
Michael L. Molino
Britney Montgomery
John S. Moore
Caryl Moore
Valerie Moran
Laura Moscove
Anita M. Moyer
Danielle C. Munksgard
Patrick J. Myers
Mercedes Isabel Naguiat
Rajni Nair
Whitney Nicholas
Michele K. Nicholl
Allyson Nieddu
Gabrielle Northrup
Deb Novak
Robert Novakowski
Alex Novoselov
Deborah Gwynn Null
Timothy O'Hanlon
Lindsay B. Ohara
Bayzid Omam
Timothy O'Meara
Christine Ondimu
Eva M. Ortea
Elizabeth A. Owen
Joanna Pachowicz
Marni L. Packy
Adriana Paladi
Mary L. Palmeri
Ethan Panek
Angela J. Parr
Tyler Parry
Mila Pascua
Dominador V. Pascual
Joseph Passoni
Nikita Patel
Krupal Patel
Josephine Patiag
Elizabeth Pavlov
Richard L. Pearsall
Lydia Perez
Jose Perich
Noah Perlman
Wesley Perry
Justin Petersen
Jean Petit-Homme
Yvette Pfeltz
Robert Phillips
Diane Piccolo
Alexandre Pinot
Walker Poppert
James Powers
Robyn Price
Ryan Quay
Malini Rao
Rashid Rashid
Christopher M. Ray
Adil Raza
Richard Rendino
Daniel Reynolds
Tracy Reynolds
Lauren Riccio

Bambi Riebesell
Meagan Ringel
Sherrie Rivera
Christopher G. Rizzo
Carolina Roberts
Olga Robinson
Mario Rocvil, Jr.
Angel Rodriguez
Diane Roman
Robert C. Ross
Teresa M. Roza
Jared Rubin
Seth Ruden
Sara Ruvic
Michael E. Ryan
Christina Sampaio
David Sanchez-Aparicio
Justinah O. Sarumi
David Terrill Sawyer
Sukhvinder K. Sayal
Elizabeth Sayre
Brenda J. Schmidlen
Tamara Schoenhals
Julie A. Schultz
Michelle Segura
Tapash Sengupta
Antony Shang
Ryan Sheen
Judith M. Sheetz
Liat Shetret
Raquel Shingleton
Natasha Shivprasad
Nadezda Shunina
Jasmine Sicular
Raheel Siddiqui
Charmian Simmons
Samuel A. Sitkowski
Raegen A. Smith
Donald Smith
Jerome Edward Smith
Elizabeth B. Smith
Clifford John Spates
Jennifer E. Speir
Logan Stair
Deborah Stanko
Elizabeth Dee Starr
James Stave
Brett Paul Steelman
Karen R. Steffens
David L. Stevens
Sandra Stevenson
Sandra Suarez
Kimberly Suchora
Dena Suftko
Lee M. Sullenger
Teresa K. Tam
Jiang Tao
Doug Taylor
Charles Taylor
Chelsey M. Telliard
Bonnie Terbush
Thomas Thampi
Nayllibi Thomas
Cheryl G. Thompson
Donald Thompson

Patricia M. Thornton
Tsedebe Tibebe
Andrew Tierney
Paula Tobar
Jim Tom
Yvette Toro-Pinzo
Robert Travers
Robert Triano
Kenneth Triemstra
Eric Trudeau
Susannah B. Truitt
Julian Tudorache
Yaroslav (Jerry) Udud
Ricardo Ugarte
Jeremy Valeo
Christopher J. Valotta
Alexandra Vasquez
Brian Geoffrey Verkest
Marlo Vibal
Stephen Vincent
Prerak M. Vora
Linda Walker
Ethan D. Wallenberg
Rebecca Wang
Ming En Wang
Lijun Wang
Keith Ward
Choya D. Washington
Joseph P. Weber
Michelle A. Weerasuriya
Jon Michael Weiner
Gregory Weissman
Susan Ashley Welch
Christopher T. Wertz
Ornetta W. White
Barry Joseph White
Lloyd White
Lawrence Wiegand
David Williams
Mike Willner
Mabel Wilson
Stephen Wong
Suzanne Wood
John Workman
Chunhao Xu
Xiao Yang
Rina Yarra
Silva Young
Juliette Zaengle
Kevin Richard Zemann
URUGUAY
Sthefani Barreto Poses
Nicolas Formager
VENEZUELA
Elvis Chirinos
VIETNAM
Hung Hoang Nguyen
ZAMBIA
Victor M. Makai
Suzyo Ndovi-Akatama



Ulrich de la Paz, CAMS
Willemstad, Curacao

Ulrich de la Paz, CAMS, has been working in the banking sector for 10 years, of which seven years have been spent in the compliance area. He is currently, the assistant compliance office manager of Maduro & Curiel's Bank N.V., the leading bank in Curacao, with subsidiaries in Aruba, Bonaire and St. Maarten. He oversees the daily AML/CTF monitoring and reporting of unusual transaction, gives support to the subsidiaries of the bank in the Caribbean region and is conducting bank wide AML/CTF/KYC training sessions.

He is CAMS certified since September 2009 and is currently the chairman of the Association of Compliance Officers of Curacao (ACCUR). ACCUR organizes seminars, lectures and panel sessions for its members and non-members to keep abreast with the current developments in the compliance field and recent threats.

Ulrich's recent accomplishment was co-chairing of the 7th CRCA conference held in St. Maarten on November 2013, where he had a terrific networking opportunity with compliance professionals in the Caribbean region. He is currently a member of the Caribbean Regional Compliance Association steering committee for the upcoming conference, as the chairman of ACCUR.



James Vaughn, CAMS, CFE
Las Vegas, Nevada, USA

James Vaughn, CAMS, CFE, is currently a senior internal auditor with MGM Resorts International, a Fortune 300 company, since 2007. Starting as a staff Internal Auditor in 2005, his time with MGM Resorts has been primarily focused on gaming and Title 31 compliance. He is fluent in the gaming regulatory requirements for Nevada, Michigan, and Mississippi and specializes in Title 31 Chapter X part 1021 (Rules for Casinos and Card Clubs). During his time with MGM Resorts he has developed multi-jurisdictional training in specific gaming activity and has an interest in understanding the use of electronic gaming devices as a means of laundering money.

He is also a co-chair of the recently formed ACAMS of Southern Nevada chapter and looks forward to working with other gaming industry professionals to help represent the industry within the wider AML/CTF community.

James has earned a bachelor's degree in Philosophy from Southeast Missouri State University, a bachelor's degree in Food and Nutrition, specializing in Hospitality and Tourism from Southern Illinois University in Carbondale, and is working toward a master's degree in Hotel Administration at the University of Nevada in Las Vegas.




Eylon Zemer, CAMS
Toronto, Canada

Eylon Zemer is currently the compliance manager at Caledonian Global Financial Services in Toronto where he also serves as a director. Caledonian has a global presence with offices in New York, Toronto, the British Virgin Islands and Grand Cayman, where it was established over 40 years ago. It has recently been awarded "Best Offshore Bank Cayman Islands" and "Best private bank" by World Finance.

Zemer plays an integral role in Caledonian's global compliance and anti-money laundering effort by providing expertise in offshore and private banking. His responsibilities involve implementing internal policies and procedures across multiple lines of business including, but not limited to banking, wealth management, securities brokerage and custody, and trust and corporate services. He is also part of the Foreign Account Tax Compliance Act (FATCA) implementation team. Zemer has previous experience in account monitoring and investigations, risk management and reporting.

Prior to his current position, Zemer spent time working directly with Caledonian's global chief compliance officer in the Grand Cayman headquarters. While in Cayman, he attended numerous banking, compliance and anti-money laundering conferences and seminars. This is something he continues to do in Toronto with the latest being the *1st Annual AML & Financial Crime Conference* in Toronto.

After having attained a Bachelor of Arts degree from Toronto's York University, Zemer went on to successfully become a Certified Anti-Money Laundering Specialist (CAMS) and is currently completing a diploma program offered by the Society of Trust and Estate Practitioners (STEP). 



Crossroads

The AML community in 2014 faces a very real crossroads. Can those in the private sector succeed in their roles without appropriate resources and consistent “tone at the top?” Will the government be able to focus on what is really important — getting reports to law enforcement or spending time assessing blame for administrative and operational deficiencies? At this stage, the answer is a resounding, “No!”

What is needed is a break from finger pointing and a return to collaboration and a seeking of the same goals — preventing, detecting and reporting criminal activity.

ACAMS is the only organization that represents all parts of the AML community throughout the globe and I continue to be impressed by the commitment of compliance professionals who try to ensure that their institutions or firms have the goal above as their priority. What else is needed, however, is dialogue and a commitment to improving laws, regulations and guidance, so that we are altogether and not divided. Look to ACAMS for more opportunities for the AML community to work together and not against one another.

Recognizing the contributions of Women in AML

We are extremely proud of this edition of *ACAMS Today* and our focus on women and their important role in anti-money laundering compliance and policy. While we cover a finite group of leaders, there were many others who excelled at developing

ways to address the criminal movement of monies. There are too many to list but several to mention include; Amy Rudnick, Whitney Adams, Marcy Forman, Lisa Arquette, Nina Nichols, Suzanne Williams, Lisa Grigg, Susan Galli and Debra Novak. I apologize for many not listed but we certainly know there were many more. A reminder that this edition is just a small tribute to the many women who are leaders in the very challenging area of compliance.

Conference challenges — Help us out

As veterans of training and other forms of programming, ACAMS takes seriously the evaluations and comments of our many participants. The difficulty in providing updated and relevant content at all of our programs revolves around targeting our audience. ACAMS programs are comprised of an audience of seasoned and entry- or mid-level AML professionals and we certainly strive to appeal to as broad of an audience as possible. Always remember that we also need to present general or plenary sessions that are both high level but timely and practical. The line we walk is to offer current information that is understandable to all no matter what the level. ACAMS continues to welcome your insight on how we can ensure relevancy to all.

For those that demand interaction, remember you are part of the program as well. We try to provide time for questions but if the scheduled time is rather compacted, seek out a

moderator before a session and offer a question. Any moderator worth their “salt” will gladly accept your assistance.

Finally, be specific in your evaluations with recommendations on speakers, format and content — we need your help.

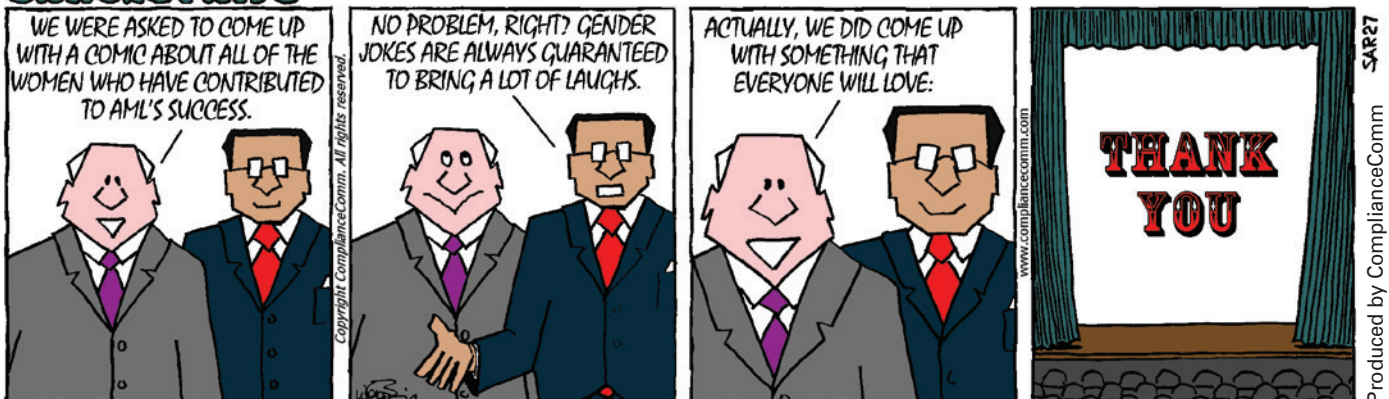
More 2014 priorities

At press time, many of you would have been contacted by a company working with us on next areas of focus for ACAMS. We will certainly review the results of that survey but it is safe to say we will continue adding to our vast array of offerings such as advanced certification, risk assessment and targeted training. ACAMS is already developing methods to address the AML-related issues such as sanctions, anti-corruption and bribery, and a deeper understanding of the various products and delivery channels that present AML vulnerabilities. One major source of covering these issues is *ACAMS Today* and the many members who provide content and guidance for the entire ACAMS community.

While other organizations say they provide support to the AML and Financial Crimes professionals, ACAMS actually comes through — by virtue of your commitment to the organization. Thank you! **A**

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

SARSnSTRIPS™



Leaving a legacy with



Jonathan Estreich



Dr. Lisa Bowyer



Nancy Lake

CAMS AUDIT

In the spring of 2013, ACAMS introduced the Advanced AML Audit (CAMS-Audit) Certification program. The first of its kind in the financial crime industry, CAMS-Audit is designed to build on the expertise of those who are already CAMS certified and bring a higher-level of specialty to their knowledge and skills. As a final assessment, each student was tasked with researching and contributing an approved white paper on the topic of AML Audit, which will be used by the financial crime prevention community to improve their compliance programs. The inaugural classes far exceeded the expectations of the Association; as the white papers started to be submitted, it was clear that these were documents that would leave a lasting impression on the community.

ACAMS Today had the privilege to sit down with three of the first graduates of CAMS-Audit to ask them why they chose the program, their experiences throughout the duration of the course and what the benefits are of becoming a Certified Advanced AML Audit Specialist. Here are three unique perspectives of CAMS-Audit graduates.

Jonathan Estreich, CAMS, CAMS-Audit

Jonathan Estreich is a vice president within the internal audit department at JPMorgan Chase. With over eight years of experience working with financial services firms such as Deloitte Financial Advisory Services LLP and UBS Investment Bank, Estreich specializes in providing anti-money laundering and counter-terrorist financing services with a focus on policies, procedures and internal controls, including those relating to transaction monitoring, Know Your Customer initiatives, customer due diligence and risk assessments. By servicing many different financial institutions within the banking sector in multiple capacities, he has accumulated a broad range of industry knowledge and expertise in diverse areas such as global AML compliance and Office of Foreign Assets Control as well as in working with complex product and customer types. He

has had considerable involvement in leading, managing and advising on BSA/AML-related matters, including authoring several works with Thomson Reuters Complanet, *ACAMS Today*, Inside Counsel and Corporate Compliance Insights. Estreich is a Certified Fraud Examiner, Certified Anti-Money Laundering Specialist, Certified Associate in Project Management, and holds an Advanced Anti-Money Laundering Audit designation.

***ACAMS Today:* What originally inspired you to earn the CAMS-Audit advanced certification?**

Jonathan Estreich: The most influential factor was that the design of the program offered two very unique benefits. First, it provided a forum for industry leaders to learn from one another and share first-hand experience. Second, it forced you to delve deeper into your existing AML knowledge base and demonstrate subject-matter expertise through developing a white paper that explored a topic of your choosing.

AT: What was the most valuable part of the CAMS-Audit experience and how did the diversity in backgrounds from the different participants help broaden your view of AML Audit?

JE: I find that when you're in a job function with intense responsibilities and high stakes, it can at times lead to tunnel vision. By its very nature, AML issues are in the spotlight, and often require urgent attention and specialized knowledge. The CAMS-Audit experience provided the opportunity to step back and reflect on this. In this setting you are no longer thinking about AML through the lens of your job function, but as a whole, and from the perspective of your peers. This type of heightened awareness can lead to a better understanding of AML risk.

AT: Your white paper contribution will help guide others in AML Audit and related areas. What was the topic that you chose for your white paper and did you consider any other topics?

JE: I considered many topics. In fact, 50 percent of the process probably consisted of choosing a direction and articulating the message.

I decided to develop a white paper that offers specific suggestions for how a financial institution's internal audit department can design a firm wide AML risk assessment tool that improves the auditor's ability to identify relevant AML risks; sets the foundation for thoughtful and supported risk determinations; and produces results that can assist in the development of an audit plan that satisfies current regulatory expectations.

AT: What piece of advice do you have for those who are considering participating in the ACAMS Advanced Certification programs?

JE: Do it. And commit. You will benefit most if you plan ahead and set aside the time. Unlike many other programs, you have an opportunity to brand yourself and develop a voice that can lead to change. By leveraging the white paper as a tool to connect with the broader AML audience, you can share insight and promote thought leadership — but it requires dedication. To assist with your work, the program offers a strong support network that wants you to succeed. It's well worth it to take advantage of that.

AT: What changes do you foresee in the AML Audit landscape?

JE: You will have to read my white paper for this one.

Dr. Lisa Bowyer, CAMS, CAMS-Audit

Prior to forming Liberty Compliance and Training, Lisa Martine Bowyer was a member of the management of the Cayman Islands Monetary Authority, and had been a consultant in the Insurance Firms Division of the FSA (U.K.) and manager in the Financial Advisory Services Division of KPMG in the U.K. She is a Certified Anti-Money Laundering Specialist and is ACAMS-Audit certified.

Dr. Bowyer was an academic for nine years with distinguished publications in the field of insurance and regulation. She is a regulatory and compliance professional both in the U.K. and Cayman Islands for over 12 years. She has a high level of understanding of the purpose, risks and models of regulation, international legal and regulatory requirements and the drivers and strategies of financial markets and products. She is also skilled in drafting of inter alia, legislation, other mandatory provisions, guidance, and policies and procedures, with an excellent appreciation of policy determining law and regulation.

ACAMS Today: Why did you choose the AML Audit career path?

Lisa Bowyer: It chose me! I was first an academic specializing in law and regulation and then a regulator. Circumstances led me to becoming an independent consultant and audit is a key service offered.

AT: What was your favorite part of the CAMS-Audit program and most worthwhile?

LB: The residential [live] course was the most valuable. I am a sole practitioner and writer, so researching and writing the white paper was not a new experience. The course, however, gave me an opportunity to work with other professionals with significant experience and yet from many different roles, sectors and sizes of institutions. This helped me a great deal in further developing objectivity and to prepare for all types of audit engagements.

AT: What topic did you choose to contribute for your white paper? Was it the only topic you considered?

LB: My topic was high-risk countries and I selected it on day two of the residential course. Whilst the scope of the paper changed once I started my research, the topic never did.

AT: How do you think the CAMS-Audit designation will help you with future changes to AML Audit?

LB: At the moment there are some differences internationally in the requirement to have an independent AML Audit. Once those are reconciled it is possible that standards for AML audit will be developed and CAMS-Audit professionals will play a valuable role in the development of those.

Nancy Lake, CAMS, CAMS-Audit

Nancy Lake has nearly a decade of experience in the BSA/AML world. Lake was CAMS certified in 2008 and as part of the inaugural class received her CAMS-Audit certification in 2013. She has served as BSA officer in multiple banks where she successfully set up the entire BSA program. She has conducted bank wide BSA/AML training including board of director training. Lake has experience working with or implementing several automated BSA/AML monitoring systems.

Lake was brought on board at one institution under enforcement action to correct deficiencies in their BSA program. She did this by implementing robust CIP processes, enhancing their reporting and monitoring programs, and developing their Money Services Business (including international money transmitters) CDD and EDD requirements. The enforcement action was lifted in six months. She has experience working with both FDIC and OCC regulators.

She joined ACBB in November 2012 as manager of the consulting arm of ACBB (Compliance Anchor) to utilize her BSA experience and 19 years as an educator to provide assistance to community banks in managing risk and developing sound internal programs and best practices.

ACAMS Today: Why did you choose to earn the CAMS-Audit Advanced Certification?

Nancy Lake: I am in the consulting business to help community banks manage the BSA burden. This burden weighs heavily on all BSA officers especially the ones wearing multiple hats with little or no help to do their job. I wanted to be certified in AML Audit to help community banks evaluate their BSA program and ensure nothing is missed in preparation for their audit.

Since CAMS certification is the premier certification in the BSA/AML arena, I knew that the CAMS-Audit certification would become the premier certification for BSA/AML audit. I wanted the best certification possible to benefit the BSA officers with whom I work.

AT: What sets AML audit professionals apart from other AML professionals?

NL: AML audit professionals have a different perspective and role than that of other AML professionals. AML audit professionals see multiple banks and AML programs and are challenged to critique every aspect of the program based on the risk profile of the bank to prepare the bank for their exam. This gives

them a deeper perspective of AML and in a sense makes them the bridge between the AML professional and the examiners.

AT: Why would you recommend earning the CAMS-Audit Advanced Certification to your colleagues?

NL: CAMS-Audit not only gives you the credentials to put after your name that are recognized worldwide, but expands your knowledge, deepens your experience and challenges you to articulate your thoughts in writing via the white paper.


AT: Speaking of the white paper, what was the topic you chose and did anything influence you to choose it?

NL: I chose the topic "What Auditors Should Know and Ask About BSA/AML Software Before a Successful Audit Can Be Conducted." Another CAMS-Audit participant encouraged me to pursue a software-based paper on our class discussions and my input, so I never really considered any other topic.

AT: What challenges do you see for AML auditors and what role will CAMS-Audit play in helping to adapt to those challenges?

NL: AML challenges continue to increase due to our constantly evolving mobile banking world and those exploiting it for their own illegal profits. Auditors will have to understand these challenges, the processes that should be in place to mitigate the risks associated with them, and have the ability to evaluate AML programs with fairness and consistency. CAMS-Audit will help to establish AML Audit standards across the globe.

Visit http://www2.acams.org/AML_Audit_White_Papers to read Jonathan's white paper on Building AML Audit Risk Assessment, Lisa's white paper on High-Risk Countries and Nancy's white paper on BSA/AML Software.

For more information about the ACAMS' Advanced Certification programs, visit: www2.acams.org/advanced. 

Interviewed by:

Catalina Martinez, advanced certification program administrator, ACAMS, Miami, FL, USA, cmartinez@acams.org

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

Phil Sobczak, marketing manager, ACAMS, Miami, FL, USA, psobczak@acams.org

INTERMEDIARY FUNDS TRANSFERS:

The **EYE** of the AML **STORM**

What exactly is the role of a bank that provides intermediary funds transfer services when it comes to investigating and reporting suspicious activity? The short answer is it is the same as any other financial institution. To those familiar with international banking, banks that provide intermediary funds transfer services are sometimes referred to as intermediary banks. This is more to define that they are one of the limited number of banks offering this type of service, as opposed to some specialized banking institution, which

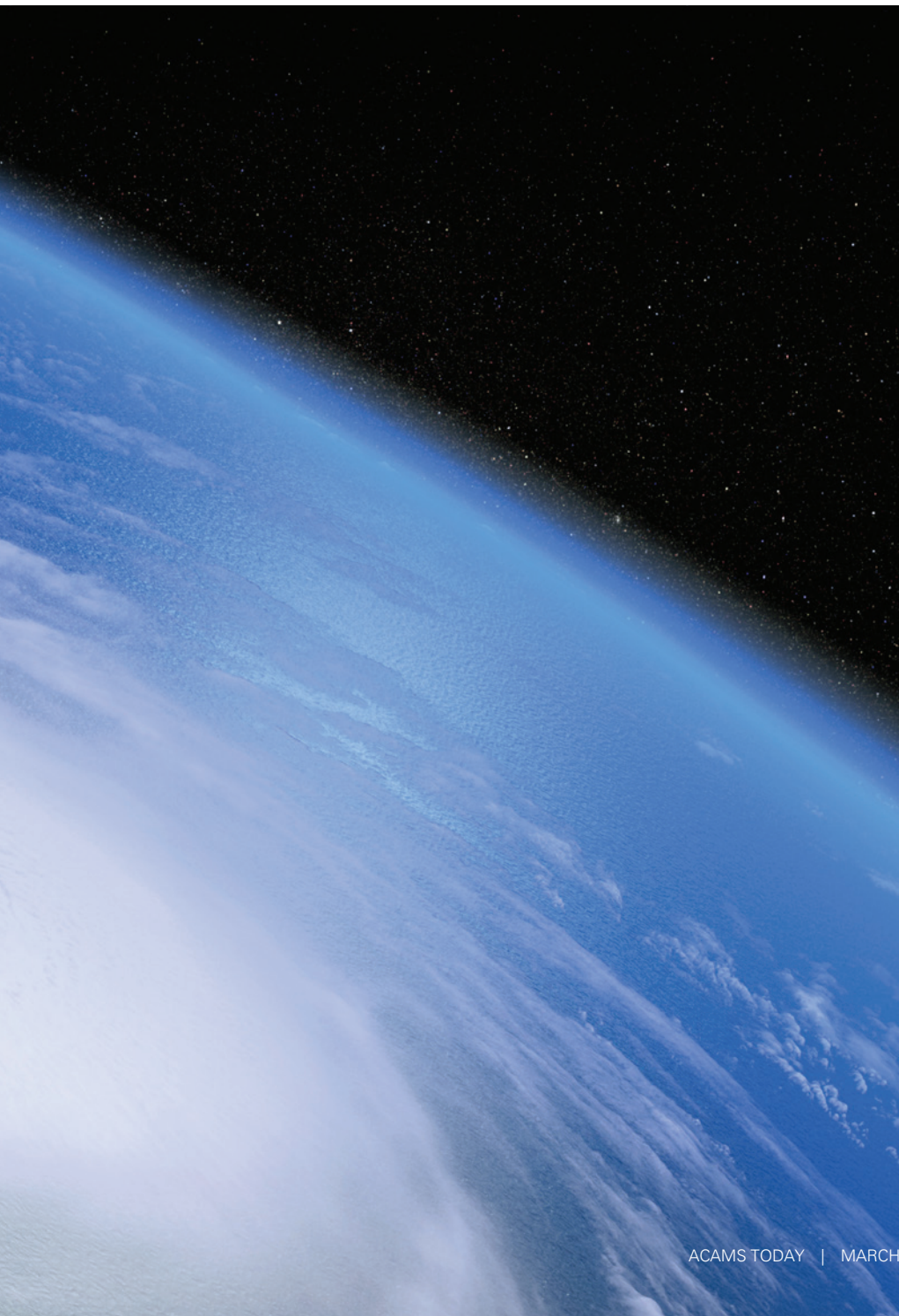
does nothing else. The service is usually just one of a number of services that particular institution provides in addition to its normal menu of products and services.

The business of intermediary funds transfers results, in some respects, from economies of scale. Going to your bank in most parts of the world and discovering they do not have the ability to send a wire transfer across an ocean would leave even the most unsophisticated consumers scratching their heads, potentially costing customers. The start-up costs, however, when coupled with

the Information Technology (IT) costs to maintain a platform for a service that may never be one of the bank's main revenue generating sources, makes seeking out an alternative a much wiser option. Accordingly, a bank will seek out another bank that has invested in the service and has the established connections. As previously mentioned, the choices are somewhat limited. The largest banks in the U.S., those with a global presence, provide the market share of the business. U.S. branches of foreign banks are also often heavily involved in the business as foreign banks seek to protect their own corner of the world and keep the business in the family, so to speak, while generating handsome fees that can be made with volume. Once established, the bank which sought assistance now becomes a correspondent bank or customer of the intermediary bank.

Correspondent banking is generally the more comprehensive term used to describe the entire relationship. So there is no confusion, the correspondent bank is actually the customer of the bank providing intermediary services, and while Know Your Customer (KYC) and due diligence is required on your correspondent bank, it is not where the day in and day out risk lies. The challenge for anti-money laundering (AML) professionals at intermediary banks is analyzing the individuals and entities who are the originators (senders) and beneficiaries (receivers) of the transaction, the customers of your customer. The originator and the beneficiary can be any of several combinations. They can include a customer of your bank, a customer of your correspondent bank or a customer of a non-correspondent bank. In some cases the intermediary bank and correspondent bank may be part of the same holding company. Under this scenario, in theory, a customer of both banks can also be considered a customer of each other. In almost every funds transfer, at least one of the participants, and often both, is not your direct customer.

Another scenario that sometimes exists is when another intermediary bank is involved. As an example, business A (the originator) needs to wire funds to business B (the beneficiary). Business A goes to their bank (Bank A — the ordering bank) which is a correspondent bank of Bank C (the sending intermediary bank). Business B's bank (Bank B — the receiving bank) is the correspondent bank of Bank D (the receiving intermediary bank). If it sounds



confusing it really is not, but you do have four banks now involved of which the general public has little conception.

While it may be a great academic argument to determine the onus on which financial institution should be recognizing and reporting suspicious activity first, as we all know, the Bank Secrecy Act (BSA) does not provide for different levels of responsibility based on a financial institution's particular role in the transaction chain. In an industry that continues to become more regulated and litigious by the day the defense of "not my job" has become nothing more than a mild euphemism for willful blindness. For an intermediary bank in the U.S., all other banks involved may not even be in the U.S., and of course not subject to the BSA. Because the transaction, however, passes through the U.S. financial system, the intermediary bank is in the eye of the AML storm, and in the peculiar position of potentially telling another bank they cannot service transactions from one of its customers; which additionally may raise a concern about that bank itself.

The least suspicious source could be the worst offender

Product and pricing compatibility

Since most international transactions will be business-to-business oriented, the initial cursory review is whether the entities involved have product compatibility. In other words does it make sense that they would be engaged in a business relationship? An example of this would be a clothing retailer making payment to an overseas garment manufacturer. The names of the two entities may initially point you in that direction, and make the review quite mundane, particularly if the entities are

larger well-established ones. By no means, however, should complacency set in, since as we all know, the least suspicious source could be the worst offender.

Another situation that will often present itself are transactions that have indirect product compatibility, such as a supplier that provides a product which is an ingredient to producing the final product; or a product that is an unrelated cost to run a business, having no connection to the product line. These are challenging and require a more complete and in-depth understanding of the nuts and bolts of the business. In today's world knowing your customer's business does not necessarily mean the customer has to bank with you or have their business records on file at your institution. While of course helpful, you can piece together enough information through the Internet and third party service providers to generally draw a picture of how a business operates.

While you can breathe a sigh of relief once satisfied that the import and export relationship makes sense, it still does not answer the question of money laundering through overpayment and underpayment. Pricing compatibility is a staple of trade-based money laundering reviews, but for an intermediary bank, with no direct customer or involvement in the transaction, determining the number of units involved and the price per unit are two obstacles which must be overcome. Like product compatibility you can utilize the Internet to obtain a ballpark cost of a unit. Finding out the number of units will require reaching out to the other banks in the transaction.

Name recognition

There is often a direct correlation between the names of entities and suspicious activity. Legitimate businesses, big and small, usually have their product or service as part of their company name — marketing 101; however, many businesses do not for a variety of reasons. Some names are the result of an entrepreneur using a catchy name that has some connection to his or her life, or something thought of in the middle of the night. For others it is a blatant attempt to obfuscate what the business is involved in. While the sending and receiving banks in different corners of the world may know their customers business, the intermediary bank will not. Names such as Worldwide, National or Global may be a harmless attempt to project a large enterprise to

impress prospective clients, but it tells you absolutely nothing; as do attention grabbing titles like Heaven on Earth, Midnight Smiles or Private Eyes, which should arouse your suspicion out of curiosity alone. Almost every business in today's environment, big or small, has a web site, but pay particular attention to pictures of corporate headquarters that give the impression of a business operating from a huge beautifully landscaped facility. A satellite view of the address associated with that same picture may reveal a broken down warehouse or mobile home. Is it someone attempting to perpetrate fraud, or just someone attempting to get a start-up business off the ground?

Keywords are a staple of processing rules to generate alerts, but flagging every descriptive adjective known to man, in hopes of discovering that one legitimate criminal enterprise would require a virtual army of investigators. Aside from standard keywords such as casino, nuclear, and jewelry, each institution should tailor their keyword search to words common to their customer base and geographic area. For intermediary banks, that can be challenging.

Country risk

A high-risk country involving a funds transfer as either the originating or beneficiary country is a standard alert and the easiest alert to focus in on. While there is nothing wrong with generating alerts when any high-risk country is involved, depending on the volume of transactions you process, the number of alerts can be overwhelming and virtually impossible to analyze — or really necessary. Of course, if both countries are high-risk, the gravity of the alert becomes that much stronger and should trigger an automatic review. The way the world is configured today you can almost take the position that the majority of the world is high-risk, but there are certain keys to hone in on.

To put it in perspective, there are high-risk countries and then there are *high-risk countries*. There is also top down corruption, where the highest levels of government are involved, and bottom up corruption, which runs the gamut from low- to mid-level government officials. Which is worse? Depends on the situation and the governments involved, but suffice it to say that top down corruption lends itself to major economic crime and violence. As for terrorist financing, that is always a concern.



A Global Presence No One Can Ignore. If you want to compete in the global economy, partner with a global leader – Fiserv. Our Financial Crime Risk Management Platform brings unique abilities for financial crime professionals to efficiently model, detect, investigate and resolve risks across crimes, channels and product lines. With 16,000 global clients in over 80 countries, you can feel confident about partnering with us. Fiserv gives your business the power it needs to excel. The power within. financialcrimerisk.fiserv.com

fiserv.

Payments • Processing Services • Risk & Compliance • Customer & Channel Management • Insights & Optimization

© 2014 Fiserv, Inc. or its affiliates.

China, for example, is considered a high-risk country; however, while the country may be plagued by corruption, it is not a lawless place where the government cannot police its people. The economy is also expanding, producing millionaires at a rapid pace. By contrast, countries high on the Failed State Index and/or the Corruption Perception Index (CPI), such as the Central African Republic, Chad and Zimbabwe, raise a further level of concern. Countries in the top 30 percent of the Failed State Index not only exhibit top down corruption, but suffer from authoritarian rule, abject poverty, human rights violations, lawlessness, genocide and sometimes civil war. On the continent of Africa, which has more than its share of failed states, exploitation of vast natural resources present an opportunity for riches, legitimately or illegitimately, answering the question of why anyone would want to do business there. To that end, top down corrupt governments need to give their blessing and that blessing has a hefty price tag. Many of these failed corrupt states have government leaders either directly involved in the nations business sector or as hidden owners. Unlike the U.S., many countries around the world are not restricted with burdensome regulations and restrictions like the Office of Foreign Asset Control (OFAC). Funds transfers to countries on the failed state list, from individuals and undefined business entities, present the biggest red flag an intermediary bank can face.

The structuring paradox

Everyone is familiar with structuring, but for an intermediary bank, funds transfers that fit the profile of structuring present an unusual dilemma. Unless the originator or beneficiary is your direct customer, or if you can somehow find out, you may never know if a cash deposit or withdrawal is part of the equation. Complicating matters is that many people, not only in the U.S., are familiar with Currency Transaction Reporting (CTR) requirements, and are under the impression that the requirement may extend to non-cash transactions, such as personal checks and funds transfers. This precipitates them to keep their transactions below the reporting threshold.

A situation can now develop, for example, whereby the originator is in Germany, the beneficiary is in Brazil and the intermediary bank is in the U.S.; but you have no way of determining if cash is involved. In some respects it is immaterial and the intermediary

bank still needs to file a suspicious activity report (SAR). You can certainly take the position that the activity is still suspicious and with no evidence to the contrary it is always better to err on the side of caution.

Wide world of cars

All international funds transfers involving vehicles should have an alert generated for review. While a system may not be able to detect every transfer involving cars, trucks and motorcycles, your alert parameters should at a minimum include the keywords; car, truck and motorcycle; and all variations such as automobile and vehicle. The major auto manufacturers control their new vehicle inventory throughout the world and black market sales affect their pricing and profitability, creating a negative domino effect on the economy. In addition to the negative effects of a robust black market, there are a myriad of other deleterious scenarios — none of them good — one worse than the other.

Recent complaints filed across the U.S. by various district offices of the United States Attorney have brought to light what had been a silent and growing cottage industry, the export of luxury vehicles abroad, particularly to China. Vehicle manufacturers, for the most part, have contractual agreements with their dealerships in the U.S. from knowingly or even unknowingly selling a new vehicle to anyone who intends to export it abroad less than one year after the purchase. The scheme is extremely lucrative since a luxury vehicle exported abroad can be sold for two to three times its cost. That's because dealerships in some countries have long delays and prices much higher than the maximum underground price. The U.S. government is alleging that fraud is being perpetrated against the dealers and manufacturers, with exporters generally using straw buyers to make purchases across the country. Why straw buyers? Bulk sales to one individual or entity may raise questions as would buyers whose ethnicity connects them to countries known as vehicle export havens. The straw buyer often tips their hand that something is up, since they ask no questions about the vehicle, pay full sticker price and forego a test drive. The exporter provides the straw buyer with the funds via cashier's check or a wire directly to the dealer's account, which in turn has brought additional charges for wire and mail fraud. The straw buyer drives the vehicle off the lot and rendezvous with a transport carrier

usually less than a mile away. From there, the vehicle is transported to a port for shipment overseas.

Now you have to question the dealer's role in all this, and have to believe that they often may have some inkling that their customer is a straw buyer based on the above Modus Operandi (MO), which is contrary to what most people do when purchasing a new vehicle. Sure, a well-schooled straw buyer can pull off the transaction giving an academy award performance as a normal customer, but the pressure to move product often outweighs common sense. If caught, the penalty to the dealer can range from fines and incentive reductions to holdbacks on inventory.

Many dealers have their customers sign a non-export agreement, which allows the dealer to penalize the buyer. Most straw buyers are hardly going to be fazed at that point about the ramifications of what could happen when they need immediate cash. How it gets enforced or if it can be enforced is another story. Until a straw buyer is jailed for fraud on that alone, it is nothing more than the proverbial dog and pony show. Another twist to the scheme has the straw buyer immediately signing the title or certifi-

You may never know
if a cash deposit or
withdrawal is part
of the equation

cate of origin over to the exporter. The intent here is to circumvent any non-export agreement, since the original owner can now claim they sold the vehicle within the U.S., rendering the non-export agreement invalid as it pertains to them. The exporter can make the same claim since they now appear as the second owner, not subject to the same agreement. The transfer of ownership also creates the appearance of the vehicle now being classified as used, which may come into play during a customs

inspection. Some vehicles are intentionally driven around the block several times adding mileage to further distort the new or used argument. To show how well thought out the scheme is, the back of most of the titles/certificate of origins signed over will usually have no odometer reading recorded. A vehicle can now be made to appear used based on mileage with a slip of the pen, adding forgery to the list of charges.

Notwithstanding the above, a litany of additional issues is part and parcel of the scheme, which includes registering vehicles in one of the five states that do not charge sales tax by creating a false residency and/or shell company, insurance fraud, theft of services of state motor vehicle agencies, money laundering through shell companies set up by the exporter and customs violations. As often happens when you either break the law or sidestep rules and regulations a separate negative consequence can result. In what may be the quintessential example of gallows humor, the transaction prevents the ultimate purchaser overseas from receiving notice of any manufacturer recall. The thought of someone driving down an icy, dark, desolate road with the brakes failing is obviously a disturbing by-product of the scheme.

Over the last several years there have also been several cases of exporters not only convincing straw buyers to become straw buyers but to finance their purchase, under the guise that the exporter will make payments until they sell the vehicle and pay it in full. The payments never materialized setting off a chain reaction of problems for everyone but the architects of the fraud, who overnight increased their profit margin by the cost of the vehicle. The bank or finance company, whoever provided the financing, quickly discovers a borrower who has no intention of paying because they were fooled themselves. Good luck trying to repossess the collateral, which may now be somewhere in China, by the Russian border or Nigeria. For the straw buyers, a civil suit for collection of the amount owed and damage to their credit rating is a further by-product of the mess; not to mention the losses to the lender. Most exporters do not go to these extremes, since angry straw buyers are a recipe for a backlash, which in these cases ultimately led to the schemes unraveling. Another variation is the straw buyer, whether acting in concert with the architect or on their own accord, reporting the exported vehicle as stolen, thus risking

the more serious charge of insurance fraud. On a limited basis this may be successful, but eventually will come to dissolve quickly. Another concern of cars exported from the United States centers on later models being stolen and carjacked. There is obviously no comparison between those who deal in deception as opposed to those who resort to physical theft and violence.

In what may be a bizarre finale to all this, some exporters are fighting back, claiming their business model does not violate any law and that vehicles and bank accounts seized by the government in the handful of cases to date must be released. There is no mention by the exporters of some of the ancillary issues that piggyback off this business model, which ultimately may lead to their undoing, even if successful with their basic defense. You would have to believe that eventually some form of legislation to protect the auto manufacturers is on the horizon.

Wider world of cars

Funds transfers revolving around exporting from the U.S. is one thing, but what about vehicles being imported and exported from other countries not involving the U.S. The 1973 film *The French Connection*, centered on the transport of heroin hidden inside a vehicle. Product compatibility, which applies to any situation, is generally the only litmus test you can apply to raise that type of suspicion, absent any additional insight or information. Going hand-in-hand with country risk as outlined above are vehicles with a final destination of a failed state. Reoccurring film footage on the nightly news over the years shows military personnel and militia groups roaming these states in late model pick-up trucks, usually with a machine gun mount. Every failed state has one thing in common, a well-off ruling class, that due to logistics and possible global economic sanctions, are willing to pay double and triple the sticker price for their personal luxury vehicles and for trucks used to dole out their interpretation of justice.

If you deem further investigation warranted relating to a funds transfer involving vehicles manufactured and sold in the U.S. there are some avenues you can pursue, which may provide you with the necessary information to reinforce or alleviate your suspicions. If you are able to obtain

the vehicle identification number(s) of the vehicle(s) involved in the transaction you can obtain a Carfax report, which will give a detailed history of the vehicle. A Carfax will enable you to track the movement of the vehicle and will also report where the vehicle was titled and/or registered. Coupled with a copy of the title or certificate of origin, which you may be able to obtain through the Division of Motor Vehicles of the state of registration, you can now draw a clear picture of what exactly is going on. Both services are relatively inexpensive, and in the case of Carfax, if your institution is involved in auto lending it can be a great tool for skip tracing the collateral of defaulted borrowers. Carfax covers Canada and has a European division also.

The intermediary challenge

In some respects the challenge for investigating suspicious transactions from the intermediary funds transfer perspective is the same as any other bank, often coming down to the drive and experience of the BSA officer, company culture and the BSA/AML budget. One of the most frustrating hurdles hampering the investigative process may be communicating with other financial institutions due to language, cultural and time differences; however, this can be overcome. Sending messages through SWIFT, a secure financial messaging system, is one avenue always available, and believe it or not, 314(b) may actually have been created for intermediary banking. Since many international wires are connected to trade settlement financing and letters of credit, should one of your customers be a party to the transaction, internal information should be readily available. There are also some excellent third party providers available that track imports and exports, which may be a worthwhile investment.

FinCEN and Financial Intelligence Units (FIUs) around the world are working in concert to thwart terrorist financing and global economic crime. The intermediary bank in the United States has a critical role in this fight as it is uniquely positioned to see transactions that others may not view or want to view as a questionable. **A**

Charles Falciglia, BSA officer, China CITIC Bank International Limited, New York, NY, USA, CharlesFalciglia@cnbinternational.com

FROM SMURFS TO MULES:

21st century money laundering

Remember those lovable blue cartoon characters, the Smurfs? First created and introduced as a comic strip series of characters by the Belgian artist Peyo (pen name of Pierre Culliford) in 1958, the Smurfs were brought to Belgian television in the early 1970s and then introduced to countries outside Belgium through the full-length feature the *Magic Flute* soon afterward. Interestingly, the word “Smurf” is the original Dutch translation of the French “Schtroumpf” which, according to Peyo, is a word invented during a meal with fellow

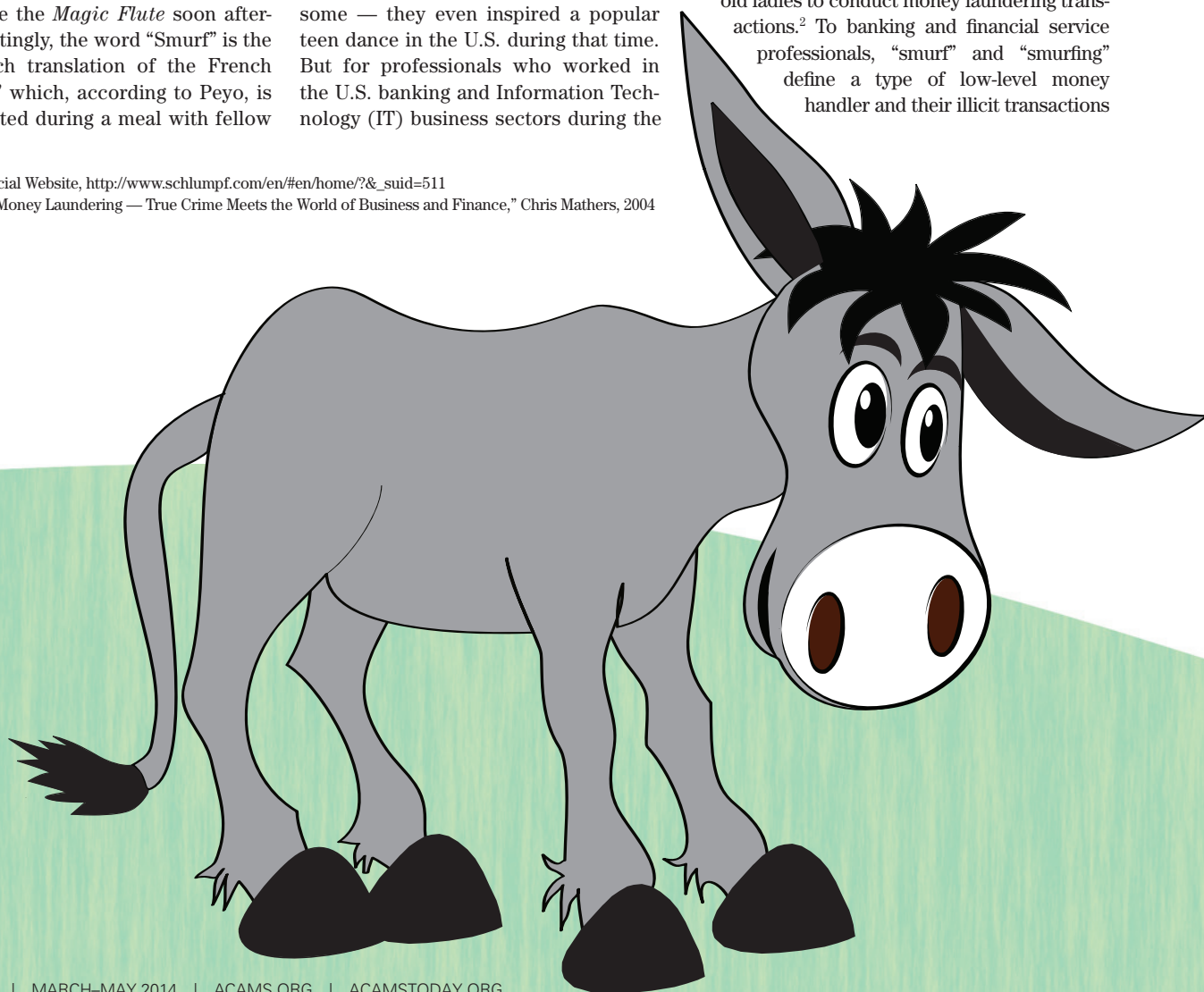
cartoonist André Franquin, when he could not remember the word “salt.”¹ The characters grew into an international phenomenon during the 1980s after the launch of the children’s television cartoon, becoming first an American then global sensation. The songs and antics of those little characters may bring back fond memories of childhood for some — they even inspired a popular teen dance in the U.S. during that time. But for professionals who worked in the U.S. banking and Information Technology (IT) business sectors during the

go-go 1990s explosion of consumer credit cards and global Internet connectivity, the word “smurf” is a word that evokes not-so-quaint connotations.

The slang use of “smurf” is purported to have originated to describe Colombian drug cartels’ use of armies of elderly “blue-haired” old ladies to conduct money laundering transactions.² To banking and financial service professionals, “smurf” and “smurfing” define a type of low-level money handler and their illicit transactions

¹ The Smurfs Official Website, http://www.schlumpf.com/en/#en/home/?&_suid=511

² “Crime School: Money Laundering — True Crime Meets the World of Business and Finance,” Chris Mathers, 2004



respectively. Traditionally, smurfs are a group of individuals who have been recruited to either max out or drain stolen credit card accounts, usually at the direction of a higher-level party who stands to benefit from the activity. Individuals or “smurf crews” are tasked to conduct point-of-sale or online retail transactions using stolen physical cards or counterfeit cards created using stolen card account data. The term has also been affiliated with persons known to one another who seek to evade currency transaction reporting (CTR) requirements by breaking up or structuring large dollar transactions into smaller transactions below the reporting threshold.³ For IT professionals the word “smurf” is likewise associated with sinister activities. In simple terms, a “smurf attack” is a type of denial of service attack in which a system is flooded with spoofed “ping” messages from multiple computers. This creates high computer network traffic on the victim’s network, which often renders it unresponsive.⁴

Large-scale global criminal activities involving trafficking and financial crimes of all types grew exponentially during the 1990s, and advances in computer technology magnified the threat to the stability of both the financial services and IT sectors. The convergence of money laundering and computer-based criminal activities is certainly not coincidental, particularly given the potential for large payoffs, the security of anonymity on the Internet, the relative ease of infiltration, and the natural barriers against capture and prosecution despite the risks. Thus, the paradigm of bank robbery changed with technological advances, and the days of physically robbing banks were over.

In hindsight, the phenomenon behind the combination of “smurfing” and “smurf attacks” to perpetrate financial crimes over the Internet was aided in part by the active push by governments and banks worldwide toward more technology-driven, globalized and accelerated financial transaction systems over the last 40 years. Unfortunately, as with any new technology developed throughout human history, advances can yield negative consequences when used to facilitate nefarious activities. Thus, while the 21st century marked the dawn of

a technology-based future, “smurfing” and “smurf attacks” became the foundations of a new-age — and arguably more menacing — money laundering technique applied by both individual and organized offenders alike: the “Money Mule” scam. Whereas smurfing was established through credit card theft and fraud, money mules answer to a similar but far higher calling: facilitating coordinated, large-dollar, and often multi-national financial crimes.

The scam

According to the U.S.-Computer Emergency Readiness Team (US-CERT), money mules are “people...used to transport and launder stolen money or some kind of merchandise. Criminals may...recruit money mules to use stolen credit card information. Individuals...may be willing participants; however, many...are not aware that they are being used to commit fraud.”⁵ For discussion purposes, the perpetrator/boss of the money mule scam will be referred to as the “driver,” and the end transactor/proxy as the “mule.”

The concept and use of mules is not new to criminal activity. The practice was established through drug trafficking techniques decades ago, whereby multiple individuals were (and still are) used to transport narcotics domestically or across international borders in small amounts fractured from bulk transactions. Money mules conduct similar tasks when structuring financial transactions. One process of recruiting and “breaking in” a new mule is simple in form, yet effective, and can work as follows:

- First, prospects are recruited by the driver through job vacancy and “work-from-home” ads using email, print media, Internet chat rooms, or job and temp-hire web sites;
- Second, the driver convinces the mule to work for their fake company and may go as far as soliciting personal identifiable information (PII) through official-looking contracts or employment forms;
- Third, once recruited and activated, the mule will receive illicit funds into their bank account;

- Finally, the mule receives instruction to remove the funds from their account and send them to another party (typically a cohort) less a commission (salary), generally using wire or automated clearing house (ACH) transfers.⁶

The extent to which this process is successful has been a direct determinant of the success of large-scale financial crime in the 21st century Internet age.

Cyber-crime mules

Herded by both cell-based and individual drivers, cyber-crime mules serve solely to enable the monetization and/or laundering of proceeds derived from criminal activities perpetrated through the Internet. The Federal Bureau of Investigation’s (FBI’s) “Operation Trident Breach,” investigated through 2009 and 2010, was a significant case highlighting foreign nationals recruited as money mules. The victims were U.S. commercial bank customers whose accounts were exploited by international cyber thieves using malware and phishing techniques to successfully steal \$70 million of a potential \$220 million in funds. The FBI charged upward of 92 individuals and arrested 39,



³ Investopedia, <http://www.investopedia.com/terms/s/smurf.asp>

⁴ The official CERT Advisory CA-1998-01, <http://www.cert.org/advisories/CA-1998-01.html>; see also Technopedia, <http://www.techopedia.com/definition/17294/smurf-attack>

⁵ 2011 US Computer Emergency Readiness Team (US-CERT), http://www.us-cert.gov/sites/default/files/publications/money_mules.pdf

⁶ US-CERT, https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf; see also Bank Safe Online (UK): <http://www.banksafeonline.org.uk/common-scams/money-mules/money-mules-explained>

most of whom were young Eastern Europe men and women who were either planning to travel to, or were already present in, the U.S. on J1 student visas. Once the suspects were in the U.S., the organizers of the mule operation gave the recruits fake foreign passports to open accounts at banks across the country. Then days or weeks after those accounts were opened, other actors in the group would transfer money from victims' accounts into the mule accounts, typically in amounts close to \$10,000. Mules then withdrew the funds, typically in amounts below the CTR reporting threshold, collected their 8-10% commission, and transferred the funds overseas. Meanwhile, other mules simultaneously conducted continuous ACH transactions through shell business accounts at high velocities, which resulted in the laundering of the funds.⁷

In this case, the mules bore the immediate brunt of law enforcement response, and although some drivers were captured through international cooperation, the template behind the crime had been laid for others to follow in future exploits.

A more recent large-scale money mule event involved international cybercriminals who perpetrated a global ATM theft in the spring of 2013 where upwards of \$45 million was simultaneously drained from hundreds of bank accounts by multiple individuals in 20 different countries over the course of several hours — \$2.8 million in New York City alone. In the case of the New York City-based ring, authorities discovered that upon completing their mission, the mules shipped the stolen cash by bus to an individual in Miami, Florida who was to then transport the funds offshore, likely to yet another proxy or the masterminds behind the crime.⁸ The participants indicted in the scam were complicit in the crime: ATM security photos detailed the dates, times, and locations of each withdrawal as the team scoured Manhattan for machines to use, and their confiscated cell phones revealed incriminating photos detailing their exploits along the way.

These are just two examples of the complexity and the degrees to which cybercriminals have exploited both financial service and IT internal control

weaknesses to maximize financial gains while retaining anonymity to avoid capture by using money mules.

Types of mules

Whether recruited as willing conspirators in the scam or unsuspecting targets of opportunity for exploitation, money mules are crucial to the successful monetization of ill-gotten gains. In another recruiting scenario, mules pre-identified by the driver as “willing” participants are engaged in the plan from the onset, provided guidance on establishing accounts, and may be outfitted with false identifications. Once prepared and equipped, they may remain on standby until given their marching orders. While the risks to both the driver and mule are many, it is the mule that faces the greatest risk as the transactor of the funds and is thus the party most susceptible to capture and prosecution.

Unsuspecting mules used as one-off pawns may have been herded through recruitment tools employed by the drivers including, but not limited to, work-from-home online, print, or targeted email advertisements and could ultimately become targets of the scam themselves. If bogus job applications were transacted using their PII, mules could fall victim to identity theft in the future should the driver and/or their associates retain and leverage this information for such purposes. Furthermore, these individuals can also suffer additional financial harm if captured by authorities, as their participation in the crime could bar them from future access to banking and financial services.

Finally, wholesale victims of identity theft suffer from both the use of their PII in the scam through the manufacture of false identification documents and the personal financial damage caused by the repurposing of their identities for money mule activities.

Organized crime links

It stands to argue that the use of money mules to facilitate financial crimes has increased to the point that their activities can now be loosely tied back to organized criminal syndicates. True to their historic pattern in other exploits, organized criminals actively seek and enter the gaps in industries and markets that promise the highest profit margins and lowest chances of investigation

and prosecution by authorities over the long haul. This long-term perspective is important when assessing the emergence of their association with money mules.

First, organized crime groups have a legendary affiliation with gambling, and their involvement in the rise of Internet-based gaming worldwide was inevitable, specifically because this relatively unregulated market promises unprecedented profits with nominal oversight from authorities. Second, with this foot hold already well-established over the Internet, the increase in sophisticated cyber-crime achievements has undoubtedly drawn organized criminals' attention, particularly considering the parallels to the freedoms and profits offered by online gaming. Third, whether through direct employment or “general contracting,” hackers' capacity to facilitate large-scale identity theft, money laundering, and fraud using “smurf attacks,” malware, and money mule networks are services that organized criminals can easily afford to either develop or retain.

Furthermore, consider cybercriminals' deep ties to former Soviet-Bloc countries and Russia itself. The downfall of the Soviet Union in 1991 left a plethora of highly educated science, mathematics, engineering, tactical military, police, and public sector computer talent with few viable legal options to sustain a general standard of living. As the once closed society struggled to move its economy into the global marketplace, the black market economy and corruption that once underpinned the Communist system continued to thrive to meet the needs of ordinary citizens. Meanwhile, this natural talent pool of black market entrepreneurs and computer experts did not languish; rather, some of these individuals seamlessly transitioned to the lucrative businesses of organized and cyber-crime. Russian criminal syndicates thus simultaneously increased in power as a force within the formal and informal Russian economy, reportedly with the aid of corrupt government officials. Investigations have determined that these organizations have come to appreciate, seek, exploit — and in the case of corrupt officials protect — the talents of home-grown hackers and cybercriminals, particularly where bank and securities fraud schemes are concerned.⁹

⁷ FBI, <http://www.fbi.gov/news/pressrel/press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring>; see also FOX News, <http://www.foxnews.com/tech/2010/11/22/cyberthieves-human-foot-soldiers-money-mules/> and Krebs on Security, <http://krebsonsecurity.com/tag/operation-trident-breach/>


⁸ Wall Street Journal, “More Arrests in ATM Cybercrime,” November 19, 2013

⁹ “Fatal System Error,” by Joseph Menn and “McMafia,” by Misha Glenny

Summary

History will someday consider the dawn of the Internet as one of the most significant technological leaps forward by mankind. Meanwhile, however, the Internet in its current state seemingly facilitates a “Wild West” environment where rules, regulations, and standards have yet to be established, especially from an international perspective. One must only consider the December 2013 mass cyber-theft of over 70 million customers’ credit card data and PII from Target retail stores in the U.S. In this case the perpetrators have yet to be identified, and early news bulletins have pointed to the fact that this information was immediately posted on underground “carder” marketplace forums frequented by cyber-thieves around the world who seek to exploit such information for credit card and identity theft purposes. Possible organized crime links to the theft have been mentioned, and other U.S. retailers were also affected.¹³ Once this stolen information is put to use, it is inevitable that money mules will be employed to monetize and distribute the bounty. Oh, for the days of “smurfing....”

Suggested reading:

- *McMafia: A Journey Through the Global Criminal Underworld and Dark Market: Cyberthieves, Cybercops, and You*, by Misha Glenny
- *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet*, by Joseph Menn
- *Crime School: Money Laundering: True Crime Meets the World of Business and Finance*, by Chris Mathers
- *Red Mafiya: How the Russian Mob Has Invaded America*, by Robert I. Friedman 

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.

Cyber-crime schemes have also been affiliated with traditional U.S.-based organized criminal groups as well as others based in countries such as Turkey.¹⁰ The extent to which this symbiotic relationship has been successful has not been fully measured to date as data continues to be gleaned from multinational investigations and prosecutions. Only time will tell the true degree to which organized criminals have migrated to the use of cyber-crime. However, given the aforementioned increases in the organization, sophistication, speed, and efficiency of cyber-crimes and the associated use of money mules, the question becomes not whether organized criminal syndicates are a part of the problem, but how deeply they are involved.

Investigations may
require interviewing
the customer to
determine the level
of their involvement

Possible money mule red flags

Although not comprehensive, the following lists possible red flags to the presence of money mule activity at financial institutions:

- Opening of a deposit account with minimal deposit soon followed by large electronic funds transfer (EFT) deposits;
 - Suddenly receiving and sending EFTs related to new employment, investments, acquaintances, etc., (especially Internet opportunities);
 - New deposit account with unusual amounts of activity (e.g., account inquiries, large dollar or high number of incoming EFTs);
 - Incoming EFTs then shortly afterward outgoing wire transfers or cash withdrawals approximately 8–10 percent less than the incoming EFTs;
 - Foreign exchange student with a J1 visa and fraudulent passport opening a student account with a high volume of incoming/outgoing EFT activity.¹¹
- Ongoing transaction monitoring initiatives targeting ATM transactions, automated clearing house and international transaction (ACH/IAT) transfers, and wires should normally trigger alerts and active responses from an institution’s Bank Secrecy Act/anti-money laundering (BSA/AML) compliance function. However, indications of the above-listed mule activities should further alert compliance officers to the possible presence of more complex scenarios warranting further investigation. In addition, if a customer’s account was unknowingly accessed by the originating transactor, the institution must consider whether their customer could be the victim of identity theft, account takeover, or hacking committed via computer intrusion and whether the incident occurred in the institution or via compromise of the customer’s online banking, email, or other computer-based activity. If the customer is a victim of these activities, then the institutions’ IT support should be made aware of the matter and coordinate with the BSA/AML compliance investigation accordingly as well as file an incident report with the appropriate regulatory authorities in accordance with SR 05-23/CA 05-10.¹²
- Investigations may require interviewing the customer to determine the level of their involvement in the transactions in question. When addressing the customer, the institution should consider treating the interaction as a discussion concerning possible suspicious activity, as the customer may or may not be complicit in what could be an account takeover wire fraud scheme that may not necessarily involve mule activity. Even if the customer states that questionable wires are valid, the transaction could still be considered suspicious if it is outside the customer’s normal and expected activity, in which case the bank should contemplate filing a suspicious activity report (SAR) should the customer truly be party to a money mule scam.

¹⁰“DarkMarket,” by Misha Glenny

¹¹FDIC Special Alert SA-185-2009, <http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html>

¹²Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12/1/05, <http://www.federalreserve.gov/boarddocs/srletters/2005/sr0523.htm>

¹³Wall Street Journal, “Card-Theft Code Grew in the Net’s Dark Alleys,” January 22, 2014

Assessing the convergence between terrorist groups and transnational criminal organizations

Looking back, the prevailing thought was that terrorists posed a threat to national security while criminal organizations primarily posed a threat to the economy. Looking forward, the landscape has changed significantly. Terrorists groups continue to pose a primary threat on national security; however, their reliance on criminal activity as a funding mechanism has also made them a threat to the economy. Traditional ethnic organized crime groups like the Italians, Russians and Asians continue to primarily pose a threat to the economy. In contrast, newer criminal organizations that thrive in areas of conflict like Afghanistan, Pakistan and Mexico pose a threat to the economy, while also posing a threat to national security. These groups have openly formed alliances with and have increasingly found a financial benefit in collaborating with terrorists.

This evolution has been driven by the financial requirements of the disparate groups. Regardless of the nature of the group — to succeed and sustain operations — they must have ready access to funding. Traditional organized crime groups have an existing financial infrastructure and long-term goals. This sense of financial stability affords them the opportunity to maintain their customary criminal activities. Conversely, newer criminal organizations tend not to have the same financial stability and are geared more to short-term goals. They function best in areas of crisis and/or conflict. This is where they find common ground with terrorists. Terrorists have lost many legitimate funding streams and, therefore, have turned to criminal activity as a main source of income. As

a result, newer criminal organizations and terrorists have realized they have much in common and have formed very profitable partnerships. This trend is one that will continue to grow.

The growing nexus between criminals and terrorists should cause law enforcement and the financial services industry to broaden their view of terrorist financing. When looking for or dealing with terrorist financing, we should assess the potential nexus terrorists might have with criminals through their financial activity.

How do you broaden the concept of terrorist financing to cover the nexus between terrorists and criminal organizations? You broaden it by looking at this emerging problem as threat finance. Threat finance is an umbrella term used to encompass various types of financing that support activities harmful to national security. The concept of threat finance was given visibility by the

Department of Defense (DOD). DOD recognized that threats to national security went well beyond terrorism. There is no singularly accepted definition for threat finance. It encompasses:

- Terrorist financing;
- Transnational criminal organizations (including drug cartels);
- Proliferation and weapons of mass destruction.

That brings us to the intersection between crime and conflict. Criminal organizations and terrorist groups have increasingly found a common ground of mutual benefit. Each has learned how to benefit from conflict through violence and crime. The wars in Iraq and Afghanistan exemplify this fact. More troublingly, terrorists and criminals have learned how to benefit from convergence and diversification.

- *Convergence* is the intersection where criminals and terrorists work together to support each other with the goal to maximize the benefit of their individual causes. They realize mutual as well as individual benefits, thus promoting collaboration.
- *Diversification* takes place as organizations mature in operations and sophistication. With maturity and sophistication, they diversify into different activities and thereby grow and strengthen their operations. These organizations rely on legitimate and illegitimate fronts to conduct business in furtherance of operations.

Terrorists and criminals
have learned how
to benefit from
convergence and
diversification



An example of a group who has benefited from convergence and diversification is the Haqqani network operating in Afghanistan. The Haqqani network is closely aligned with the Taliban. They are the most diversified and well-organized component of the Afghan insurgency from a business perspective, occupying key spaces in both licit and illicit economies in Afghanistan and Pakistan. There are many other criminal organizations, who like the Haqqani's, have benefited from close associations with terrorist groups.

An important commonality shared by criminal organizations and terrorists is their reliance on corruption. To be able to operate with impunity in regions of conflict, ungoverned regions and in regions with more stability, terrorists and criminal organizations rely to a great extent on corruption. In looking at the Haqqani model, they operate in Afghanistan and Pakistan, two of the most corrupt nations in the world. Officials they deal with in that region are more interested in their personal enrichment than the best interest of their countries. Corruption, transnational crime and terrorism form a dangerous trifecta.

Transnational criminal organizations

Transnational criminal organizations (TCOs) pose a serious global economic threat. They also represent an increasing threat to U.S. security and interests both domestically and internationally. TCOs carry out criminal operations across international borders. In that sense, they rely on financial facilitation tools to support cross border activities. Such mechanisms include bulk cash shipment, wire transfers, correspondent banking, trade-based money laundering and the use of shell companies. Their interest in the "bottom line" makes them more dangerous. If they believe anyone poses a threat to their ability to raise and move money, they will react violently. TCOs are typically located in countries with weak rule of law, thus allowing them to operate freely. These organizations pose a significant threat to regional security where they operate and they thrive on conflict. Exacerbating the threat to regional and national security is the willingness of TCOs to work with and provide material support to terrorists.

Drug trafficking is one of the most prolific and profitable criminal activities that TCOs and terrorist groups engage in collectively and individually. Successful drug trafficking operations require increased levels of corruption. Drug trafficking also leads to

regional violence and instability. In addition, it causes health and social issues. Other criminal activities that TCOs and terrorist groups engage in collectively and individually include: arms trafficking; human smuggling and trafficking; product counterfeiting; trafficking in contraband; sea piracy; kidnapping and money laundering.

As noted earlier, illicit networks pose a threat to both national security and the economy. Their use of violence and intimidation poses a threat to national security. Their engagement in criminal activity poses a threat to the economy. Corruption is an important key to success for these networks. It acts as an enabler that facilitates their operations. As illicit networks look for new areas to exploit, cyber security has become an increasingly significant threat.

Terrorist-criminal nexus

The crime-terror nexus includes two independent, but related components:

- The involvement of terrorists in criminal activities as funding sources, and
- The linkage between criminal organizations and terrorist groups.

The evolution of the convergence of TCOs and terrorism emerged at the end of the cold war. World events at that time caused conditions that challenged the financial system of terrorism. Terrorists experienced a diminishment in their funding streams. The evaporation of funding sources encouraged and continues to encourage terrorist groups to develop into "narco-terrorist" organizations. Terrorists have increasingly engaged in drug trafficking and other illicit organized criminal activity to acquire money and material in order to sustain their organizational operations.

TCOs and terrorist groups share many operational and organizational similarities and characteristics. They often learn from each other. In so doing, they tend to imitate each other's successes and failures. Because of their similarities, TCOs and terrorist groups can easily work together and therefore frequently partner with one another. What has taken place is the transformation of illicit groups into hybrid criminal/terrorist entities. The nexus between TCOs and terrorist groups has become increasingly complex and sophisticated.

As a result of the development of these hybrid criminal/terrorist entities, especially as they become complex and sophisticated,

the public and private sectors must develop new methodologies and strategies to deal with the problem of convergence. Understanding the crime/terror nexus is the first step toward solving this growing problem.

Similarities between TCOs and terrorist groups include:

- They are generally rational actors
- They are extremely violent, especially with their propensity for kidnapping, assassinations and extortion
- They are highly adaptive, innovative and resilient
- They defy the state and the rule of law
- They pose a global threat to national security and the economy
- They possess resources ranging from leaders, backup leaders and foot soldiers
- They tend to provide social services, particularly terrorists such as Hizballah
- Others

TCOs and terrorist groups have compatible organizational and operational characteristics. They tend to adopt similar methods in terms of characteristics and tactics. However, it is important to note that they strive for divergent ends. Both require revenue and financial support to sustain their organizations and operations. For transnational terrorists, criminal activity supports their political and ideological objectives. As terrorists engage more and more in criminal activities they develop the greed factor, which can blur their sense of ideology. For TCOs, organized crime is conducted primarily for economic ends. TCOs have an inherent greed factor and it is important to point out the greed factor. Greed is a vulnerability that can be exploited by law enforcement and financial services sector investigators.

Organizational mindsets

When looking across the spectrum of TCOs, there is a clear divergence between organized crime groups. Longstanding TCOs and newer crime groups have very different relationships with terrorist groups. The defining line between these groups is the end of the cold war. Longstanding groups were formed well before the cold war ended. The newer groups evolved after the cold war.

Older groups possess long-term financial strategies. They are dependent on long established states, where they have operated for many years. These groups usually reject

associations with terrorists. These traditional older groups possess different strategies and motivations that are not conducive to collaboration with terrorists. They have well-established criminal operations and have built infrastructures in established states, mostly through corruption. With maturity, traditional TCOs have diversified into multiple licit and illicit activities. These older groups rely more heavily on the formal financial system.

Traditional TCOs include:

- The Italian/Sicilian mafia
- Russian and Eurasian organized crime
- Japanese Yakuza
- Chinese Triads
- West African criminal organizations

There is a growing nexus between criminal organizations and terrorist groups

These groups share a number of commonalities. They are longstanding, well-established and diverse organizations. Traditional TCOs operate in long-established countries. They are not associated with terrorist groups. These groups are violent, rely on corruption and conduct licit and illicit activities.

Newer groups do not possess long-term and efficient financial strategies. They often originate in ungovernable regions. The newer groups take advantage of the chaos of war and dysfunctional states. They generate huge profits from cooperating with terrorists. These groups share more consistent interests with terrorists that are conducive to collaboration. Newer TCOs have short-term and less-established operations. Newer groups operate best in states in conflict. Like older groups, they rely on corruption to safeguard their enterprise. As they mature, newer groups begin to develop diversified activities. They tend to operate in informal or shadow economies.

There are many newer TCOs. Some of the most notable include:

- Los Zetas drug cartel (Mexico)
- Joumaa drug trafficking/criminal organization (Lebanon)
- D-Company (Pakistan)
- Haqqani network (Afghanistan)

The newer groups named above grew rapidly and share a number of commonalities. They are maturing quickly and are becoming diverse. These four groups operate from countries that have been in conflict. They have profited considerably from their affiliation with terrorists. Like the traditional TCOs, these four groups are violent, rely on corruption and conduct licit and illicit activities.

Case study: Lebanese Canadian Bank

The Lebanese Canadian Bank case is symbolic of the convergence between TCOs and terrorist groups. This case study demonstrates how criminal, drug trafficking and terrorist organizations collaborated in a multi-billion dollar global narco-terrorist drug trafficking and money laundering enterprise. It was a mutually beneficial operation that involved the Joumaa drug trafficking/criminal organization, the Los Zetas drug trafficking cartel, and Hizballah, the most profitable and best organized terrorist group in the world. The Joumaas and Hizballah operate in Lebanon and are closely related, much like the Haqqani network and the Taliban in Afghanistan. The Los Zetas are the most successful and treacherous drug cartel in Mexico. This criminal enterprise succeeded by exploiting financial institutions, facilitation tools, financial mechanisms and other systemic vulnerabilities. The Joumaa organization laundered as much as \$200 million per month. This case also illustrates how money laundering is essential to successful criminal enterprises.

Factors that facilitated the operations of the criminal enterprise included:

- The Lebanese Canadian Bank
- Money exchange houses in Lebanon
- Bulk cash shipment/smuggling
- Cross border wire transfers
- Correspondent banking
- Payable through accounts
- Shell companies/front companies
- Corruption
- Structuring

- Money laundering, to include trade-based money laundering and black market peso exchange

The Lebanese Canadian Bank sent 329 wires to correspondent banks in the U.S. totaling \$329 million. The funds were used to purchase used cars in the U.S. that were shipped to West Africa and sold. The proceeds from the sale of the used cars were sent back to Lebanon for the Joumaas and Hizballah. The wires to the U.S. were also used to purchase consumer goods in Asia. Those goods were shipped to Colombia and converted to pesos to pay Colombian and Venezuelan suppliers and the Los Zetas.

There were three funding flows in this case. The above mentioned, where money was wired to the U.S. to purchase used cars that were shipped to West Africa; the above mentioned, where money was wired to the U.S. and then to Asia to purchase consumer goods; and the proceeds from drugs sold in the U.S. that were laundered by the Joummas and returned to the Los Zetas in Mexico.

Conclusion

There is a growing nexus between criminal organizations and terrorist groups. The convergence of these entities continues to become more complex and sophisticated. As they mature, these groups are becoming diverse. This convergence and diversification presents a challenge to both the public and private sectors. In addition, the unholy trifecta of corruption, transnational crime and terrorism exacerbates the challenge to the public and private sectors.

To counter the threats posed by TCOs and terrorist groups, the public and private sectors must develop new methodologies and strategies to deal with the problem of convergence and diversification. Understanding the crime-terror nexus is the first step toward solving the problem. In simple terms, methodologies and strategies must be developed to exploit the vulnerabilities of TCOs and terrorist groups. Their principal vulnerabilities are finance, communications and greed. Finance and communication can be traced and used to disrupt, dismantle and prevent. Greed leads to arrogance, which leads to loss of focus and reasonableness. Finance, communications and greed can be easily exploited. They represent fatal flaws for criminals and terrorists. **■**

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

A “C” change for virtual currency



In the world of virtual currencies, 2013 became the year that saw the introduction of typical financial institution lexicon into the virtual world. Terms like “FinCEN,” “MSB,” “KYC,” “AML,” “BSA,” became part of the conversation. In March, participants in the virtual currency ecosystem were put on notice and virtual exchanges and administrators were urged to register as money services businesses (MSBs) with the U.S. Treasury’s Financial Crimes Enforcement Network (FinCEN) and implement proper anti-money laundering (AML) programs and controls.

Other events soon followed to ensure that virtual currency users, administrator and exchangers were aware that the regulators are reviewing what they are doing in their efforts to protect the U.S. financial system from illicit actors. High profile events such as the seizure of funds for international Bitcoin exchanger “Mt. Gox,” closure of the centralized currency “Liberty Reserve” in May, the FBI’s case against online vendor “Silk Road” in the summer, and the November hearing on virtual currencies by the United States Senate Committee on Homeland Security and Government Affairs. Given this regulatory attention, virtual currencies like Bitcoin were finding their way into popular media and part of the new digital vocabulary of the general population.

Virtual currencies

For discussion purposes, a virtual currency is a medium of exchange that operates in the digital space that can typically be converted into either a fiat (e.g., government issued currency) or it can be a substitute for real currency. There are basically two types of virtual currencies—centralized and decentralized. Centralized virtual currencies (e.g., Liberty Reserve) have a centralized repository and a single administrator; whereas decentralized (e.g., Bitcoin) has no repository or administrator but works as a peer-to-peer medium of exchange without any need for an intermediary.

Virtual currencies go beyond the most popular version, Bitcoin, with alternative currencies (otherwise known as alt currencies) that seek to expand the global virtual currency footprint. In total, there are more than 160 virtual currencies in the market. Much like Bitcoin, these currencies are mined to produce the currency for circulation. Mining is the process of spending computing power to process transactions,

secure the network, and keep everyone in the system synchronized together. Mining can also be performed through a process called “pooling,” which uses the collective computing power of many users to create coins. Once coins are created, based on previously agreed to terms of those participating in the pool, the coins are distributed to the miners. In either process, miners earn coins for their efforts. Thus, coins are created and available for circulation. Each coin has a pre-defined maximum circulation. For example, Bitcoin has a maximum amount of 21 million, whereas the leading alt currency, Litecoin, has a maximum circulation of 84 million.

The currencies can be used for trading through an online exchange whereby one trades a coin for a fiat currency or coin for coin. At this early stage in the ecosystem, Bitcoin is the premier currency and most widely used in virtual transfer. However, it is and still should be considered a high-risk instrument until the market matures. While Bitcoin may be the first into circulation and is facing numerous headwinds in the global market, this may permit the little known alt currencies to thrive in the long-term.

FinCEN’s guidance on virtual currencies

FinCEN’s March 18, 2013 interpretative guidance on virtual currencies categorizes the participants within the ecosystem into three segments—User, Exchanger, and Administrator. A User is a person that obtains virtual currency to purchase goods or services; an Exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency; and an Administrator is a person engaged as a business in issuing a virtual currency, and who has the authority to redeem such virtual currency.

Under a typical transaction scenario, a User would have an established virtual wallet or an account with an exchanger to conduct a transaction. The User would then acquire virtual currency from the Exchanger, which would allow the User to transfer funds in and out of that account.

In short, Bitcoin uses a public key cryptography algorithm to generate public and private keys or Bitcoin addresses that would allow the User to receive (public) or send (private) Bitcoin payments. To make a payment, the User (Buyer) would identify goods or services for purchase and through

the User’s virtual wallet’s private key, initiate the transaction request with the private key (a digital signature unique to the User) of the seller’s virtual wallet. The payment order information is then distributed to the Bitcoin network where the network miners verify that the buyer is indeed the current owner of the Bitcoins being transferred. Once confirmed, the transaction is then recorded in the block chain (historical records) and the product is delivered. This payment exchange process is not reversible.

FinCEN’s guidance requires administrators and exchanges to register with FinCEN as MSBs. Thus, as MSBs, such virtual currency exchanges are required by law to maintain an effective AML compliance program under the Bank Secrecy Act (BSA) and USA PATRIOT Act.

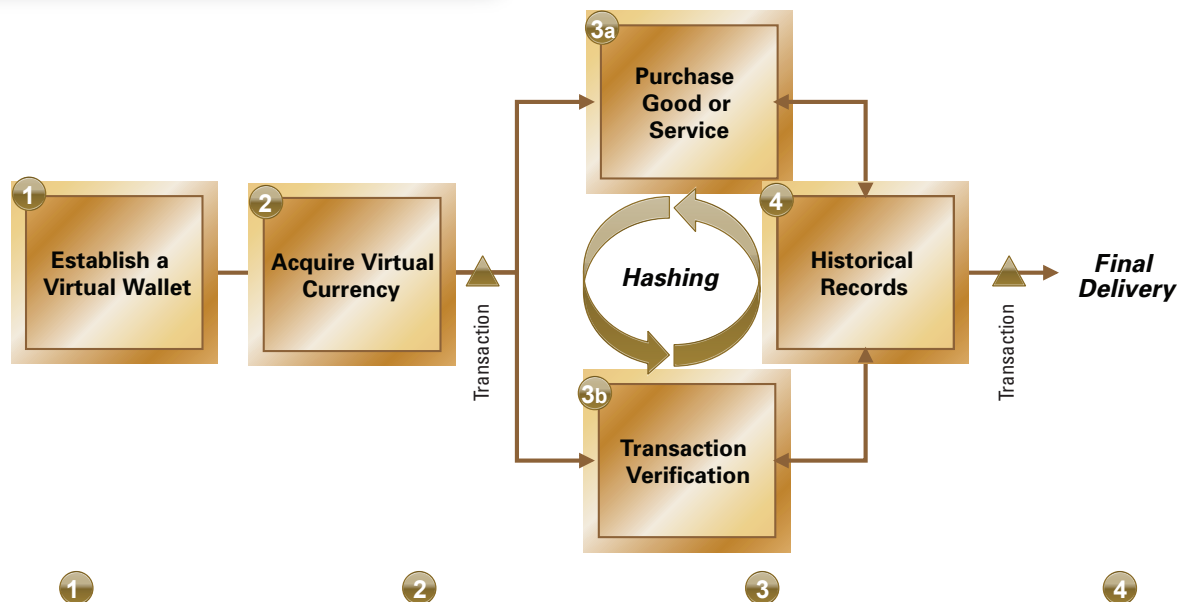
Money services business and Bank Secrecy Act compliance requirements

Under the BSA, each AML program must be commensurate with the risks posed by the location, size, nature and volume of the financial services provided by the MSB. An effective program is one designed to prevent the MSB from being used to facilitate money laundering and would include the four pillars of AML as its core components: (1) internal controls, (2) designated compliance officer, (3) training, and (4) independent testing. The “Four Pillars of AML” are known concepts to traditional financial operators, but they are relatively new in the virtual space due to the early adoption of the virtual currency ecosystem.

A “C” change for the virtual currency industry

FinCEN’s guidance created a fork in the road for product development-focused virtual currency companies. On the one hand, those that were self-funded start-ups with minimal capital faced significant challenges to maintain business operations. Individual entrepreneurs realized the cost of compliance was prohibitive. Venture capital backed companies now needed to obtain additional funding rounds that included compliance costs in the equation.

“Compliance” became more important to survival than the actual product developers were seeking to take to market. Those in market were somewhat ‘discovered’ outside the Bitcoin community and

**1 Virtual Wallet:**

Files that provide access to virtual currency addresses. Open source software available for desktop and mobile across Mac, Windows, Unix, iPhone, and Android.

2 Virtual Currency:

Exchanges handle deposits and withdrawals in which buy orders are matched with sell orders. Transfer funds into, out of, and between exchanges.

3 Transaction:

Buyer identifies goods or services and the Virtual Wallet's private key initiates the transaction request with the private key of the seller's virtual wallet. "Miners" bundle transactions into "blocks" to confirm payment and receive 25 Bitcoins for services.

4 Historical Records:

In order to modify future transactions, historical records would have to be addressed first due to randomized cryptographic numerical values added to transaction results.



faced numerous questions about their AML compliance programs. All of a sudden, notoriety resulted in too much attention to stay below the radar. Simply passively registering with FinCEN as an MSB and putting together a homemade AML policy were no longer viable business strategies. As a result, financial institutions, upon identification of virtual currency companies now designated as MSBs, elected to terminate relationships with virtual currency companies. However, those that recognized the "C" was a requirement of doing business, obtained a competitive advantage in the ecosystem.

Negative news for virtual currencies: Good? Or bad?

One of the initial main draws for virtual currencies, including Bitcoin, was their anonymity. Over several months, the front pages of online news sites were flooded with an ever-evolving series of bad press or was it really good press? Unlicensed money transmitters, seizures, online drug marketplaces, Bitcoins for hitmen—oh my! Several enforcement actions that took virtual currencies from the shadows to the homepages were Mt. Gox, Liberty Reserve, and Silk Road, which then resulted in two days in Senate Hearings.

1. Mt. Gox seizure

In May 2013, a seizure warrant was issued to Dwolla, an Iowa-based online payment processor for e-commerce, for the accounts of Mutum Sigillum LLC, the U.S. subsidiary of Mt. Gox, the world's largest Bitcoin exchange that operates out of Japan. At that time, consumers could purchase Bitcoin by depositing funds with Dwolla, and then the funds were directed to Mt. Gox for the actual purchase of the Bitcoin.

Mt. Gox acts as a digital currency exchange where customers open accounts, which are then exchanged into digital currency, exclusively Bitcoin. Account holders can fund and withdraw accounts, hence a bidirectional exchange. Accordingly, Mt. Gox and Mutum Sigillum were operating as unlicensed money transmitters in the U.S. Thus, under the BSA, the companies were required to register as a MSB with FinCEN and establish and maintain an effective AML program consisting of the four pillars.

In June, Mt. Gox registered with FinCEN and continues to operate as the leading digital currency exchange in the world. On October 28, Dwolla terminated activity with

Bitcoin and its virtual currency exchanges due to uncertainty and confusion around virtual currencies.

2. Liberty Reserve shutdown

In May 2013, FinCEN issued a Notice of Finding under Section 311 of the USA PATRIOT Act that Liberty Reserve S.A. was a Financial Institution of primary money laundering concern. Later that month, the U.S. shut down Liberty Reserve, a website operated in Costa Rica, engaged in using digital currency (its own called "LR") for payment processing and money transmission. The three-part indictment included charges for conspiracy to commit money laundering, conspiracy to operate unlicensed money transmitting business and operation of an unlicensed money transmitting business. Further, it stated "the defendants deliberately attracted and maintained a customer base of criminals by making financial activity on Liberty Reserve *anonymous* and *untraceable*" [emphasis added]. According to the U.S., the site was used primarily to launder the proceeds of illicit activity.

Liberty Reserve maintained more than 200,000 customers in the U.S., yet never registered with FinCEN. Moreover, Liberty Reserve required users when opening an account to provide basic identifying information, however, in contravention of Customer Identification Program requirements, did *not* require users to validate their identity information, therefore, accounts could be (and were) opened easily using fictitious or anonymous identities. Essentially, unverified account holders could use the site to transfer the digital currency, LR, between other unverified accounts holders.

Accounts were funded using exchangers, third party entities that maintained bulk quantities of LR that were purchased using traditional funding methods. The exchangers operated as unlicensed money transmitters. Technically, the design was to layer funds from the point of origin (traditional funding such as cash or wire transfers) through the exchangers into a digital currency, and then the digital currency could be used to purchase illicit goods or just withdrawn out of Liberty Reserve using a *different* exchanger. To add to the layering, account holders had the option to pay a “privacy fee” of \$0.75 per transaction to shield their account number when transferring funds. Unverified users plus a nominal fee to add anonymity to transactions screamed open season for illicit activity.

Moreover, in FinCEN’s Notice of Finding, it identified that Liberty Reserve “has only a statement in its policy, with *no implementation* to address anti-money laundering concerns or requirements...” [emphasis added]. Collectively, all these factors demonstrated Liberty Reserve was seeking to avoid AML compliance requirements and retain users’ anonymity.

On October 31, 2013, one of the co-founders of Liberty Reserve, pled guilty in a New York court to operating an unlicensed money transmitter, conspiracy to operate the same, and conspiracy to commit money laundering, among other charges.

3. Silk Road seizure

Following a two-and-a-half year investigation, the FBI arrested Ross Ulbricht (a.k.a. Dread Pirate Roberts), the alleged founder and operator of the Silk Road marketplace, in September 2013. Silk Road was a “dark web” e-commerce site only accessible through a “Tor” network, a network designed to an Internet user’s location or usage. Upon login, visitors were presented with a site

home page, which listed several categories of merchandise available for sale on the site. Items available for sale included controlled substances, weapons, services such as computer hacking, stolen identification information, and hitmen, to name only a few. Silk Road costumers were able to provide payment for these goods and services in Bitcoin to conduct transactions.

Moreover, to enhance anonymity and assist with laundering illicit proceeds, the site used a ‘tumbler’ to process Bitcoin transactions in a manner designed to frustrate the tracking of individual transactions through the block chain. The tumbler obscured any link between a buyer’s Bitcoin address and the vendor’s Bitcoin address where the Bitcoins end up; thus eliminating the benefit of the block chain, such as a traceable record of the transaction. However, because the government was able to seize Ulbricht’s laptop at the time of his arrest, it now has access to Silk Road’s transaction records and can trace the Bitcoin movement through the block chain and identify the exchanges and administrators that were part of the transaction process. This became evident on January 27, 2014, when two U.S. based Bitcoin exchange operators, Charles Shrem, chief executive officer of NY-based BitInstant and Robert Faillea, operator of Florida-based BTCKing, were arrested on suspicion of money laundering.

In the seizure, the FBI seized more than 174,000 Bitcoins from Silk Road and Ulbricht. The FBI contends that Ulbricht was arrested for engaging in money laundering, narcotics trafficking, and computer hacking. The trial against Ulbricht is pending. Yet, Ulbricht has filed a civil claim in connection with the forfeiture to retain the Bitcoins on his computer network.


4. Bitcoin goes to the Hill

Silk Road appeared to be the tipping point on the national stage for the government to finally want to talk publicly about virtual currencies. On November 18, 2013, the U.S. Senate Committee on Homeland Security and Government Affairs held a hearing titled “Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies.” The hearing consisted of two panels: the first from three federal agencies (FinCEN, Department of Justice, and the Secret Service); the second panel included

the International Centre for Missing and Exploited Children, the Bitcoin Foundation, and other market participants.

The virtual currency hearing was the result of several months of investigation on the topic by the Committee and was “to explore potential promises and risks related to virtual currency for the federal government and society at large.” The hearing, planned since August, received heightened interest after the Silk Road marketplace’s closure. While the federal agency participants fell short of providing full endorsement of virtual currencies, they testified that they were paying attention to the risks to the U.S. financial system and that, by and large, current U.S. regulations are adequate for charging criminals misusing virtual currencies and repeatedly referred to the requirement for virtual currency exchanges and administrators to register as money services businesses.

The swarm of press from the spring to the fall kicked the dust off of virtual currencies and created a gray cloud about Bitcoin. Was this the end of the line for the freewheeling currency? Or was it just “cleaning out the system?” for brighter days. The Bitcoin market certainly reacted with a spike in Bitcoin price in April of \$266 to the weeks following the November U.S. Senate Hearings where Bitcoin surpassed the \$700 mark. In January 2014, when the U.S. announced the forfeiture of 29,655 Bitcoins that were located on the Silk Road server with an approximate value of \$28 million, the existing exchange rate was \$933.

In the late fall 2013 and into winter 2014, Bitcoin became a payment option for spaceliner Virgin Galactic, online retailer Overstock.com, online gamer Zynga, and the NBA’s Sacramento Kings for ticket purchases, among others. In several months, Bitcoin went from law enforcement centric press to e-commerce that general consumers can relate to. Just like when the population was a skeptic of the Internet as something unfamiliar and obscure, it has become a foundation for commerce and communication. 

Brian Stoeckert, CAMS, CFE, chief strategy officer, Coin Comply, New York, NY, USA, bstoeckert@coincomply.com

Timothy O'Brien, MBA, consultant, Financial Services Volunteer Corps New York, NY, USA, timothykobrien@outlook.com

Regulators 'doubling down' on their scrutiny of casinos

Imagine a financial institution with a floor plan spanning many acres. It hosts thousands of patrons from all over the world, with points-of-transaction scattered every few feet and cash changing hands nearly each moment. Then, mix in alcohol, entertainment and, on occasion, loud, combative and inebriated guests. Obviously, no reasonable bank would operate in such a way, but all the above make for a typical casino experience, and the modern-day casino is a financial institution in every sense of the word.

Casinos have the capability to transfer significant amounts of money across the world. Large sum payouts and deposits occur regularly. Many casinos even offer safe deposit (or front money) services for clients. Perhaps, most importantly, casino operators' anti-money laundering (AML) compliance programs are now under the same intense regulatory scrutiny that other financial institutions have faced for years.

In September, FinCEN Director Jennifer Shasky Calvery addressed the Global Gaming Expo, intimating that gaming was firmly in the Financial Intelligence Unit's

Part of the caché
of gaming is being
able to sidle up to
a table and play

(FIUs) crosshairs. "Laws, rules, and compliance manuals can only do so much. A truly robust AML framework...requires effective AML program implementation by financial institutions that understand what is at stake not only for them, but for the financial system as a whole. Those casinos that do choose to ignore their AML obligations and operate outside of the law are going to be held accountable. FinCEN will act to stop abuses of the U.S. financial system."

The point was loud and clear: Casinos must know their customers and improve their own AML compliance regimes, or regulators

will take action. Treasury's perception of the gaming industry is that operators have skated for too long without truly taking their Bank Secrecy Act (BSA) obligations seriously. Shasky's comments, and subsequent actions taken by Treasury, made it known that there would now be zero tolerance for shoddy compliance work.

This all comes at a dynamic time for the gaming industry. There has been significant expansion outside of the U.S., particularly in Asia. Overseas, properties are now contributing more than 70 percent of global revenues to the gaming conglomerates. While profits are as sky high as they have ever been, some leading operators are embroiled in controversy related to financial crimes compliance. In October, it was revealed that Caesars Palace, owned by mega-casino operator Caesars Entertainment Corp., is being investigated by the Treasury Department for money laundering. The revelation comes on the heels of Las Vegas Sands agreeing to give up \$47 million to avoid criminal charges over failing to report suspicious activities.



Photo credit: Samot/Shutterstock.com

It is true that casinos face an especially daunting task in trying to keep tabs on considerable foot traffic that spends and wins in an atmosphere that is strategically designed to be as accommodating as possible. No gamblers want to be continually asked for personal information. Part of the caché of gaming is being able to sidle up to a table and play.

But it is also true that casinos likely do the best job of any financial institution in terms of gathering information. Big wins have strict reporting thresholds and surveillance on the floor is detailed. In her comments, Shasky admitted that casinos have certain Know Your Customer (KYC) elements down to a science (e.g., clients' personal preferences). However, as any AML specialist will tell you, KYC is just the start of an effective compliance regime.

The problem lies in the guidance; or more precisely, lack thereof. Regulators must understand that while banks and money services businesses have decades of experience fine-tuning their compliance programs, this is new territory for the casino industry.

To this point, requirements have been clear-cut and evenly applied, and most casino operators fared well on their regulatory exams. In the past year, that has changed. Requirements have become more stringently applied, but advice by regulators has been wanting. Regulatory supervision is becoming stricter, with greater demands for compliance and harsher terms of enforcement, all without the clarity of how best to employ enhanced AML compliance. The government wants casinos to conduct more effective enhanced due diligence, but in the context of an entertainment complex, what exactly does that mean?

Generally, when FinCEN or regulators identify an area of focus within the BSA — submission of electronic forms, Bitcoins, or changes to Foreign Bank Account Reporting forms, to name a few recent items — working groups within the agency will get together to promulgate guidance.

In 2012, FinCEN published a guidance dealing with frequently asked questions about record keeping, reporting and compliance for

casinos. That guidance, not even two years old, is outdated.

To be sure, it is the responsibility of gaming companies — who, despite a plethora of regulatory attention, still draw healthy profits — to comply with the law. The argument can be made that casinos are a front-line in the fight against money laundering and terrorist financing. If FinCEN truly wants to take the dirty money out of casinos, they would do well to explain their expectations. And for their part, casinos can do more, such as improving their suspicious activity report writing, training floor personnel to identify red flags and simply improving transactional record keeping, while also starting to share information with other operators. **A**

Vasilios Chrisos, CAMS, ACAMS global advisory board member, is a principal in Ernst & Young LLP's Fraud Investigation & Dispute Services (FIDS) practice, vas.chrisos@ey.com

The views expressed are those of the author and are not necessarily those of Ernst & Young LLP.

FATF TAKES AIM AT 7 *'Hawala Myths'*



Common perceptions about *hawala* “do not necessarily match the reality” of how the informal value-transfer system operates in North America and Western Europe, according to a recent Financial Action Task Force (FATF) report.¹

The October 2013 report is based on member countries’ responses to a 47-question survey fielded in September 2012, as well as input from a November 2012 typology workshop.² The report notes that participating countries identified seven so-called “*hawala* myths” that reflect outdated assumptions about *hawala* and other similar service providers, or, in FATF parlance, HOSSPs.³

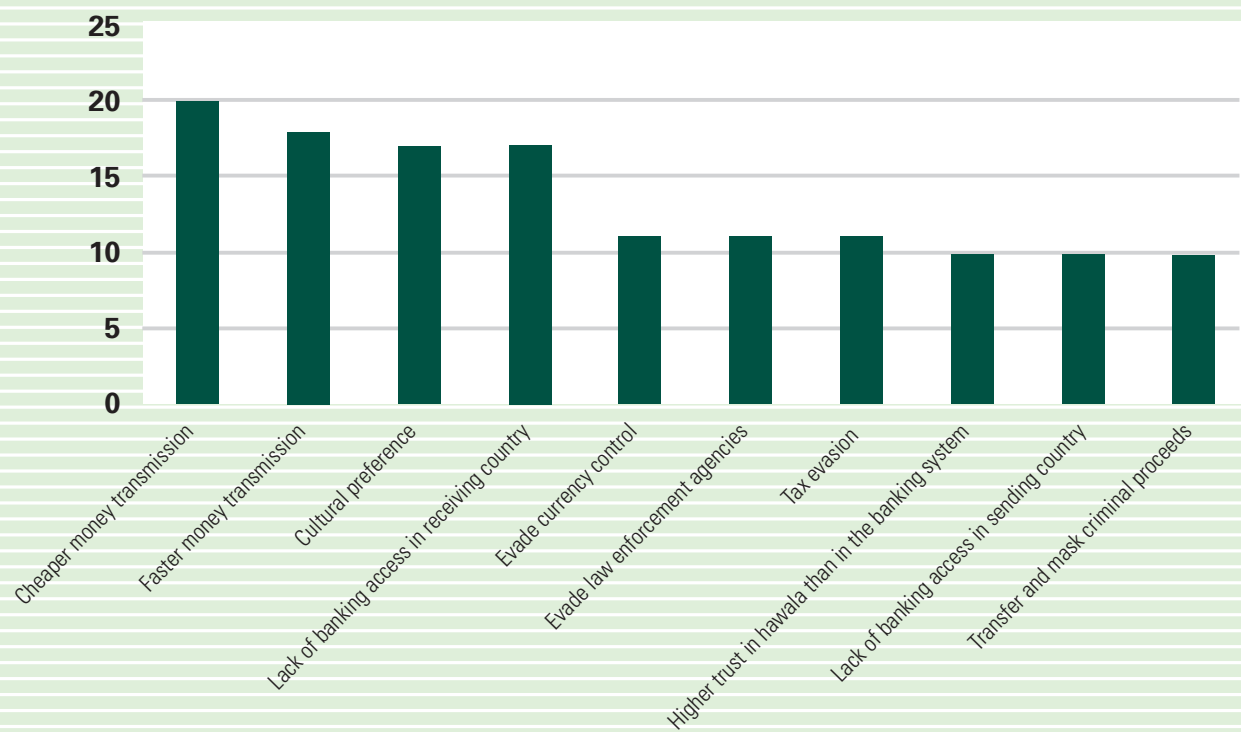
Those “myths” include the ideas that *hawala*:⁴

- focuses exclusively on transmitting remittances;
- is a paperless system;
- operates underground;
- is a trust-based system;
- invariably is cheaper than conventional banking systems;
- has remained largely unchanged over the centuries; and,
- always poses a high-risk for money laundering and terrorist financing.

Diversified entrepreneurs

Hawaladars often also engage in currency exchange, trade finance, short-term lending and other services, according to the report, which notes that for many of these entrepreneurs, money transfer is an ancillary service offered on the premises of their main business, such as a pawn shop, grocery, travel agency or mobile pawn shop. Engaging in a variety of financial services makes it easier for *hawaladars* to settle accounts with one another and harder for law enforcement to trace individual transactions, the report notes.⁵

Figure 1. Explaining the Persistence of *Hawala* and Similar Services



Source: FATF

When FATF asked member countries participating in its survey on *hawala* and similar service providers why these informal value-transfer services continue to have appeal in the modern banking era, cheaper money transmission was the reason most often cited. (Each of the 22 respondents could provide multiple answers.)

¹ Financial Action Task Force (FATF). “The Role of *Hawala* and Other Similar Service Providers in Money Laundering and Terrorist Financing.” (Paris, October 2013), 19.
² Ibid., 12.
³ Ibid., 19.
⁴ Ibid., 19-20.
⁵ Ibid., 19-21.

The FATF study observes that in *hawala*, operators typically engage in net settlement of multiple transactions that occur over a set period. “At times, *hawaladar* and other similar service providers that owe debt to corresponding providers settle accounts by fulfilling commercial obligations of such corresponding providers, such as paying a debt or invoice of the same value,” the report notes.⁶ In other cases, under- and over-invoicing is used to square accounts, FATF observes, adding that there is an even more ominous component to the interplay of *hawala* with other enterprises: “By running an additional business such as a travel or ticket agency or freight forwarding, criminal HOSSPs can derive an additional benefit that provides them with a ready supply of customer identity documents, which can be ‘hijacked’ and used to generate false customer records.”⁷

The report also challenges the notion that *hawala* transactions are marked by scant communication, with only cryptic symbols or code words employed. “Many *hawala* investigations have revealed that *hawaladars* and similar service providers actually keep detailed records. They maintain manual accounts, ledgers, computerized records or a combination of these. The businesses of some *hawaladars* are based on small margins of profit, and recording and tracking deposits, payments, and transfers is important to their good reputation and efficiency.”⁸

A not-so-secretive service

Meanwhile, the supposedly underground nature of *hawala* may be largely in the eye of the beholder, according to FATF. The Task Force explains that while *hawaladars*, who tend to serve members of a specific immigrant community, may not be readily identifiable to the larger society and its government agencies or financial institutions, they often “are actually highly visible within the community they serve and may even advertise their services openly (even when they are not a regulated or licensed or registered business).”⁹

The supposedly underground nature of *hawala* may be largely in the eye of the beholder

Similarly, the report notes that while there often is a perception of *hawaladars* as shadowy figures, they instead “are often relatively respected individuals within their communities.”¹⁰ This is important, FATF adds, because while *hawala* frequently is characterized as a “trust-based system,” it is more accurately described as being “reputation-based,” with the selection of providers based on a reputation for effective delivery of services, rather than blind trust in a member of one’s ethnic group.¹¹

While acknowledging that *hawala* and similar services typically charge only 25 percent to 50 percent of the equivalent bank fee for transmitting money, the report notes that, “Their competitiveness is highest where customers need to send money to areas where traditional banking systems and large money transmitters’ chains find it difficult, expensive, or a high risk to operate. When such conditions are not met, the cost of sending funds through *hawala* and other similar service providers may actually not be that competitive.”¹²

Hawala: Hard to define, harder to quantify

The report also points out that while *hawala* in many ways remains true to its ancient origins as a trade-finance method for merchants in the Middle East, South Asia and Africa, it is not a static system, and continues

to adapt to modern times and technologies.¹³ This fluidity makes it difficult to provide a precise definition of *hawala*, according to FATF, which noted that the term “is traditionally associated with a money transfer mechanism that operated extensively in South Asia many centuries ago and had strong links along traditional trade routes in the Middle East and parts of East Africa. It operated as a closed system within corridors linked by family, tribe, or ethnicity.”¹⁴

Recently, the report observed, *hawala* has been used as a sort of short-hand phrase to describe informal or unregulated money-transfer systems. In some cases, there is a connotation of illicit activity; in other cases, the term is not at all suggestive of illegality. In other regions, the terms *hundi* and *underground banking* are used to describe roughly the same activities as those encompassed by *hawala*.¹⁵

In the interest of clarity, FATF coined the abbreviation HOSSPs — for *hawala* and other similar service providers — and defined HOSSPs as “money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time.”¹⁶ It added, “While HOSSPs often use banking channels to settle between them, what makes them distinct from other money transmitters is their use of other settlement methods, including trade, case, and long-term net settlement.”¹⁷

While FATF managed to construct an abbreviation and definition broad enough to describe informal value-transfer providers, it refused to make any estimate of their numbers, stating flatly that, “The scale of unregulated *hawalas* is unknown and is impossible to generalize.”¹⁸ Of the 21 FATF member countries responding to a survey question about the extent of unregulated *hawalas* within their jurisdiction, most declined to venture an approximate number of such services. While some said that unregulated operations might represent up

⁶ Ibid., 16.

⁷ Ibid., 21.

⁸ Ibid., 19.

⁹ Ibid., 20.

¹⁰ Ibid.

¹¹ Ibid.

¹² Ibid., 17, 20.

¹³ Ibid., 19.

¹⁴ Ibid., 12.

¹⁵ Ibid.

¹⁶ Ibid.

¹⁷ Ibid., 13.

¹⁸ Ibid., 25.



Analytics for banking

Detect and deter
money launderers.

SAS® Anti-Money Laundering delivers dynamic risk assessment, so you investigate only meaningful alerts. High-performance analytics and multiple detection methods offer you complete protection and enable you to meet compliance demands with greater speed and accuracy than ever before.



Read the paper
sas.com/alert



to 50 percent of the money-transfer market, former FBI agent Dennis Lormel and other law enforcement sources say that in many jurisdictions that require registration of *hawalas*, the number of unregistered operations far exceeds the number of those that have complied with the law.¹⁹

The FATF report noted that in the U.S., FinCEN conducts an outreach initiative to identify unregistered money services businesses and, where appropriate, to inform them of applicable regulations and assist them in the registration process.²⁰ At the beginning of this year, more than 36,000 money services businesses, or MSBs, had registered with FinCEN.²¹ While these figures encompass traditional money-transfer agencies as well as *hawalas*, they reflect a considerable year-over-year increase in registrants.

The final assumption the report addresses concerns the degree of risk associated with *hawala* and similar services. FATF identifies three types of HOSSPs — “pure traditional,” which regardless of their registration status are not involved in illicit transactions; “hybrid traditional,” which provide legitimate services, but which wittingly or unwittingly are also involved in illicit transactions; and “criminal” HOSSPs,” which knowingly and often exclusively engage in money laundering and related illegal activities.²² FATF notes that the risk profiles may differ significantly between and even within each type.²³ Despite those distinctions, FATF member countries remain concerned about HOSSPs, with 86 percent of survey respondents saying that they view HOSSPs as being vulnerable to money laundering risk and 81 percent saying they see the services being vulnerable to terrorist financing risk.²⁴

Red flags for financial institutions

The FATF report noted that transaction patterns that may indicate that a financial institution’s customers are providing illegal or unregulated money-transfer services include:

1. “Frequent deposits by multiple individuals into a single bank account, followed by international wire transfers and/or international withdrawals through ATMs.”
2. “Money being transferred at regular intervals to international locations such as Dubai. Dubai is a major international clearing house for remittances and other value transfers. Many trading companies/criminal groups route their money through Dubai to other destinations” via *hawala*.
3. An account in which funds are transferred out almost immediately after being transferred in.
4. Frequent international wire transfers to countries or companies with no apparent business connection to the sender.
5. “Business accounts used to receive or disburse large sums but [that] show virtually no normal business-related activities, such as payment of payrolls, invoices, etc.”
6. “Frequent deposits of third-party checks and money orders into business or personal accounts.”
7. “A sudden change in pattern of financial transactions from low-value international fund transfers to large-value transfers by a money remitter.”
8. A customer frequently conducting transactions that fall just beneath thresholds for currency transaction reports (CTR) or other reporting or due diligence steps.²⁵

While the FATF report did not endorse specific recommendations, it did cite the main reasons why HOSSPs continue to pose risks for money laundering and terrorist financing. Most of those reasons were intrinsic to some or all informal value transfer systems, such as settlement across multiple jurisdictions through value or cash outside the regulated financial system, the use of net settlement, and the comingling of licit and illicit funds.

Number of unregistered operations far exceeds the number of those that have complied with the law

But the report laid primary blame for the continued risks associated with *hawala* not with the *hawaladars*; however, it was to those charged with protecting the integrity of the financial system. In the report’s assessment, “The most significant reason for concern is a lack of supervisory resources and commitment to effective regulation.”²⁶ Building support for providing adequate resources and a sustained commitment to that effort may depend, in part, on ensuring that legislators, policy makers, financial industry leaders, and others, possess a more-nuanced and comprehensive view of *hawala* as it actually operates today.

Note: The FATF report, titled “The Role of *Hawala* and Other Similar Service Providers in Money Laundering and Terrorist Financing,” is available at <http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf> 

Tom Garry, CAMS, a member of ACAMS Editorial Task Force, is the president of Exponent Communication in Hawthorne, NJ, USA, thomasmgarry@gmail.com

¹⁹Ibid.

²⁰Ibid., 62.

²¹United States Department of the Treasury, Financial Crimes Enforcement Network (FinCEN). MSB Registrant Search Web Page. Accessed January 13, 2014 at http://www.fincen.gov/financial_institutions/msb/msbstateselector.html.

²²Financial Action Task Force (FATF). “The Role of *Hawala* and Other Similar Service Providers in Money Laundering and Terrorist Financing.” (Paris, October 2013), 10.

²³Ibid., 20.

²⁴Ibid., 28.

²⁵Ibid., 57,58.

²⁶Ibid., 41.

One expert's assessment of 'Hawala Myths,' risks and responses

The man who organized and led the FBI's terrorist financing section in the wake of the September 11 attacks agrees with the FATF report that more needs to be done to reduce the money-laundering and terrorist-financing risks associated with *hawala* and similar services. However, he says the challenge isn't so much one of discarding outdated assumptions as it is of bringing sufficient focus and resources to bear.

"I think that illegal money remitters represent one of the biggest money-laundering challenges facing the U.S. financial system, despite institutions' best Know Your Customer (KYC) efforts," says Dennis Lormel, CAMS, whose long career in the FBI included service as agent in charge of the Bureau's Financial Crimes Program and, in the immediate aftermath of 9/11, forming and overseeing the government's multi-agency Financial Review Group, which quickly determined how the hijackers had funded their operation. "If people at banks are being absolutely honest, they will acknowledge that one of their biggest concerns is being able to identify customers who are engaged in illegally transferring money for others," adds Lormel, who today advises financial institutions on fraud prevention, anti-money laundering initiatives, and similar matters through his Lansdowne, VA-based consultancy, DML Associates.

In Lormel's experience, law enforcement agencies, regulators, and executives at most financial institutions already have an accurate, up-to-date understanding of *hawala*. "For example, when we were investigating *hawaladars*, we knew that they kept fairly detailed records," says Lormel, who retired from government service in 2003. And while those records might not meet generally accepted accounting principle (GAAP) standards for presentation of financial information, they were decipherable to the practiced eye. Similarly, he adds, law enforcement and regulators long have recognized that *hawala* often is entwined with trade finance, currency exchange, and the like, while bankers realize that *hawala* is not a purely separate channel but one that frequently intersects with conventional financial systems, albeit often in camouflaged fashion.

"While the 'outdated assumptions' that FATF cites may still be issues for the general public, I think these things are pretty well known in government and financial circles," says Lormel, though he adds that awareness of the situation doesn't necessarily equate with having the tools to adequately address it.

He notes that while FinCEN has made great strides in registering *hawaladars* as money services bureaus, or MSBs, the majority of such providers in the U.S. continue to operate in an unregistered, unlicensed and, thus, illegal fashion. Lormel says that while technological innovations, banks' pursuit of immigrants' business, and the extension of formal financial services to the "unbanked" overseas may help diminish the customer base of illegal *hawala* services over time, there will always be a demand for such services. "People who are here illegally are going to be reluctant to use registered services. Even though their transactions are for legitimate purposes — to send money home to their families — they may fear using a registered MSB because of their immigration status."

For Lormel, the challenge of illegal money remitters requires a multi-pronged solution that starts with bringing as many as possible into the formal system, with its licensing and registration, and accompanying record keeping, KYC, CDD, SAR and CTR requirements. Helping financial institutions "set their filters" to identify potential illegal remitters is another key step, such as increasing awareness of the indicators outlined in "Red Flags for Detecting Illegal Money Transfer Providers." Finally, an aggressive investigative and enforcement approach to illegal remitters is in order, notes Lormel, who emphasizes the importance not only of investigations that originate within the U.S., but also of taking advantage of arrests made and intelligence gathered overseas to identify the U.S. correspondents and confederates of foreign criminals.

—Tom Garry, CAMS


WOMEN IN AML: A BEACON TO THE COMMUNITY

Since the United Nations first celebrated International Women's Day on March 8, 1975, countries and organizations around the globe have joined together to commemorate "the acts of courage and determination by ordinary women who have played an extraordinary role in the history of their countries and communities" (Source: UN web site). As ACAMS reflects on this year's theme "Equality for women is progress for all," we would like to salute the Women in AML for their outstanding contributions.

These women have made history through their determination to make the world a safer place through their roles as AML and CTF professionals, and are paving the way for a younger generation of female leaders to continue the fight against financial crimes.

Throughout this edition you will find articles and interviews highlighting some of the most dedicated women in the field; from an article on Human Trafficking by Anna Rentschler, recently appointed to the ACAMS advisory board, to an interview with Suzanne Williams, who graciously provided a window into her life at the Federal Reserve Board. You will also learn about several new entrants to the community, as they share their thoughts on how they envision making a difference in the AML field. And although not formally highlighted, we also would like to take the opportunity to congratulate Janet Yellen, who at the time of press for this issue, is slated to be the first woman to take the helm as the Chairman of the U.S. Federal Reserve by taking office February 1, 2014.

The Women in AML are relentless and fearless in deterring the expansion of transnational crimes such as the financing of terrorism, the trafficking of narcotics, human smuggling, and much more. Please join all of us at ACAMS to honor, salute, and thank them for standing up in the fight against financial crimes.

For more information on International Women's Day visit: <http://www.unwomen.org/en/news/in-focus/international-womens-day>. 

Nancy Saur, CAMS:



The energizing field of AML

Nancy Saur's career reads like a road map to success — compliance and risk manager for a multi-national company, entrepreneur who co-founded a successful compliance consulting firm, and founder of the Cayman Islands Compliance Association — but she still talks about AML and compliance with the passion and enthusiasm of someone just breaking in to the field. Instead of discussing her many accomplishments, Saur talks about new challenges, learning, growing and the need to give back to the community she loves.

Saur was recently named head of compliance with Advantage International Management (Cayman) Ltd, a leading Cayman Islands-based provider of specialty insurance and related services to business owners and high net worth individuals seeking customised insurance solutions for their risk management and financial planning needs. In this position, Saur is responsible for compliance, risk and FATCA activities across the Advantage group.

We had a chance to talk with Saur recently and the following are her thoughts about her career, the industry and advice she has for others in the field.

ACAMS Today: In addition to your very busy career, you are also involved in the ACAMS advisory board and have been involved as a

mentor of compliance professionals, and facilitator of compliance education over the years. What keeps you energized and so involved in the industry?

Nancy Saur: The short answer is that it's challenging and energizing, and many times it is just plain "fun." This field has energy to it. I started my career in research and development and I enjoy researching and applying what I learned. After my first research assignment I told them, give me a problem and I will solve it.

There are many, many challenges in compliance. I enjoy defining solutions to the challenges. It tests your abilities to solve them, to find ways to minimize risks. The field is always changing. It's always expanding. There are always new challenges. Those are the things that keep me passionate.

AT: You had a long and very successful history in the banking compliance industry, including your tenure as the compliance manager at Millennium bcp Bank & Trust, why did you decide to move in to the insurance field?

NS: For the challenges it offers. It's a very exciting time for the company I am now with; it is a new stage of development for them. So, it's an opportunity to get in on the ground level of this development and bring what I know to the table. The new directions for the business bring new challenges for me to see

how I can contribute to their already strong compliance culture. Also, this is another opportunity to learn. You should never stand still and never think you understand it all.

AT: During your career, you have held a number of high-level compliance positions including being the compliance and risk manager for the Caribbean and Asian offices of the ATC Group and co-founder of a successful compliance consulting company that worked with financial services clients in the Cayman Islands, Caribbean and Central America. What first started you on your career path?

NS: I had a different career path and ended up in AML. I started with research and development and then went to audit, which got me involved in rules and requirements and best practices.

For me the transition was really kind of natural. I grew up in a household where there were rules and organization. I think that it is ingrained in me and it's part of my personality. When I got involved with compliance, I thought this is really cool, I can do this!

AT: It sounds like the compliance field is a perfect fit for you, but have you found it difficult as a woman to move forward within this industry?

NS: I've not found it difficult personally. I think for me it was because I was one of the first (as the industry was coming into its own field in the Caymans) and I took a lead role immediately. I started the compliance association and I had the knowledge to back it up. Credibility opens doors. You need to do your job well and keep yourself up-to-date.

AT: You have a strong commitment to giving back to the industry. The Cayman Islands Compliance Association is a good example of your commitment. How did you get it started?

NS: To get started I had a small network of people I reached out to and they reached out to others and we expanded, then we expanded and then we expanded some more. Everyone agreed that this was something needed in the compliance field. We were among the first compliance associations in the region.

I do what I can to give back to the community and I would recommend that everyone get involved and give back. It is only by being involved that you can learn who you can lean on and who can lean on you. Who you can counsel and who can counsel you. It is important.

I've found that the people who are most successful are those who are involved in the first place.

AT: You seem to embrace challenges. What has been your biggest challenge and what did you learn from it?

NS: One of the biggest challenges is coming to grips with a new environment. You need to understand the culture of the organization, the scope of the job and make it your own. You also need to get your internal network established. Identify who your champions will be and who your detractors will be. It is important to understand the culture of the environment and build your own internal infrastructure.

AT: What advice would you give to others starting out in the field?

NS: Get to know your local compliance community. In Cayman it is easy because we are such a small community. You can get to know your local intelligence unit, go to lunch with your regulators and law enforcement. I know in other places that it isn't possible. But you can build relationships with folks from law enforcement that deal with financial crimes. AML is going to involve financial crimes and these relationships are important.

In larger communities, it will certainly be more difficult to emulate our "home town" type of networking. But that doesn't mean you stop looking to build your network. In terms of degrees of separation, I have been able to build relationships with some really amazing people in this industry, and utilize that network to benefit from their counsel and guidance.

Also continue to learn. I think the CAMS certification and new advanced certification programs are wonderful opportunities.

AT: Finally what do you think is one of the secrets to success in this industry?

NS: First enjoy what you do. You have to love what you do in this particular business. If you don't, it affects the whole environment, and in turn affects everything.

You need to keep your head down, your nose clean and get to work. But remember that you also have to raise your head and look around. Always look out for opportunities to get involved and opportunities to share. **TA**

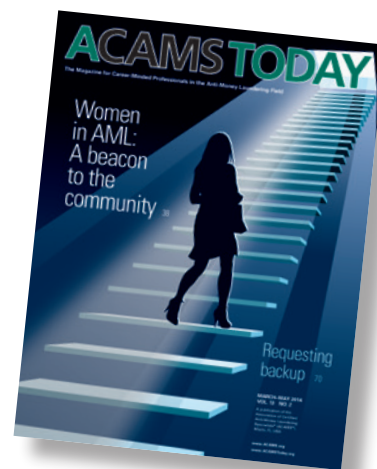
Interviewed by: Debbie Hitzeroth, CAMS, BSA/OFAC compliance officer, United States Postal Service, Washington D.C., USA, deborah.l.hitzeroth@usps.gov

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



Industrial Strength Offerings for

Sanctions & PEP Screening, KYC / CIP and Identity Verification

**Handles Unlimited
Record Volumes**

100% SaaS Up-time

**Verified Disaster
Recovery Plan**



*Available as licensed or
hosted (including interactive
web services calls), desktop,
and appliance*



*11 billion+ hosted
transactions per year*

Built upon Innovative Systems, Inc.'s (ISI) 45 years of data matching expertise, FinScan's "intelligent" linking technology **minimizes**

- ✓ **the risk of missing real matches (false negatives)**
- ✓ **the volume of false matches (false positives)**
- ✓ **the time and cost required to research potential matches.**

- Integrates smoothly with all leading third-party PEP databases
- Helps ensure the accuracy and validity of SWIFT and other payment transaction processing
- Provides sanctions lists and 24/7/365 list management service
- Integrates with selected scanners to import information from driver's licenses, passports, and other forms of government I.D.
- Automates review process through an integrated case management tool
- Facilitates customer onboarding
- Screens available in English, Spanish, French, German, and more
- Plus many other features, including document attachment

www.finscan.com



Global Headquarters - USA
+1.412.937.9300 x8237
info@innovativesystems.com

EMEA Headquarters - London
+44 (0) 20 7422 6310
infouk@innovativesystems.com

***FinScan is proud to
support Women in AML***

Celebrate March 8 - International Women's Day

PITTSBURGH • TORONTO • MEXICO CITY • LONDON • FRANKFURT

How can you not?



end it

Supervising a Bank Secrecy Act/anti-money laundering (BSA/AML) Financial Intelligence Unit (FIU) for all the banks in our holding company is a full-time job that I love. I have always had a strong liking for the BSA/AML area, but when I was exposed to the Human Trafficking (HT) element, it became my passion. I have often been asked, “How did you get involved in your interest in human trafficking?” My answer was and is, “How can you *not* get involved? How can you *not* report unusual happenings? *How can you not?*”

The topic of human trafficking was introduced to me several years ago through a coalition-sponsored meeting involving

law enforcement and a newly formed Human Trafficking Coalition. I saw a huge hole in the knowledge of the local law enforcement and citizens of the community and in comparison, the very few coalition members that were trying to affect change and knowledge in mid-Missouri. In light of this, I became involved in bringing this heinous crime to the attention of citizens, and groups both locally and nationally. The general perception from the groups is twofold: (1) This is an international issue and does not concern us and (2) It cannot happen to me, in my part of the United States, and especially in the smaller towns.

When I heard these comments, this reemphasized a *huge* need for the education regarding HT. Generally when I get through speaking, there is an eerie quiet in the room as I have usually made them aware of this hidden problem that they now embrace. Then the questions start: “Does this happen here? Can it really happen in small towns? In our community? I thought it was just international immigrants? How can we help educate local law enforcement and those around us? Has it happened here? You mean my children/grandchildren could be victims? I thought it was just prostitution, and I learned that slave labor is all around us? How young?” These are some of the starting questions because

it hits them personally and in their community, and also because they do not want it in their neighborhood. The awareness starts to seep into their thoughts and fears. That's when I know they understand the scourge of HT and that they want to prevent this from ever touching their life and the life of others. When they invite me back to continue the conversation, I know I have advocates that want to make sure we are educated enough to stop this blight.

After speaking, I have had audience members tell me that they know that they have seen this type of activity before, but did not know it had a name and what to do about it. As a response to their concern, this is what you should do if you suspect HT. First and foremost, if you witness or suspect an HT event, call 911 as soon as it is safe to do so! In addition, I always recommend that the HT toll-free hotline be called: 1-888-373-7888 or you can also text BeFree (233733). It is operated 24/7 and addresses all HT events for the entire country. Take out your cell phone (we almost all have them now) and save this number in order to have it ready in case it is needed. I have mine under: HT ICE (In Case of Emergency), so it can be brought up quickly in a search on my cell.

If you get home and realize that a report needs to be made, an anonymous tip can be made utilizing the computer form at: <http://www.polarisproject.org/what-we-do/national-human-trafficking-hotline/report-a-tip>.

Will you ever know if your tip leads to the arrest of a handler/pimp or helped rescue a HT victim? Probably not, but can you sleep at night if you remain silent? All are anonymous and chances are you will never know whether your tip led to saving someone; however, it may be the one tip that points law enforcement in the right direction. Let the professional law enforcement officers do their work; do not take it into your own hands.

My recommendation for all banks and employees is to spread HT education.

- Educate your staff. If you educate the front line and employee contact personnel on HT, they will call you or file an internal incident report if they suspect unusual HT potential or activity.

- Have a meeting with local banks or through your banking associations. Enlighten them and get them on the road to educating their staffs.
- Volunteer to speak to civic organizations and bring this issue to their attention.
- And lastly, read books and look up HT on your computer. Stay engaged and current on issues of concern in your area. Google: HT and your state, the links will surprise you due to their numbers.


"Human trafficking is a hidden crime — and every one of us needs to know the indicators to look for." The Department of Homeland Security,¹ through its Blue Campaign is just one of the excellent resources easily (and free) accessible to you to train with regarding HT, as well as many others (<http://www.dhs.gov/blue-campaign/awareness-training>). One of the resources to help bring it home (and kudos to them for doing so) is the Michigan Law School at the University of Michigan. Their Human Trafficking Database launched in February 2011 "hopes to strengthen anti-trafficking laws in the United States..." It is an ongoing project that supports all who are involved "who are working on behalf of human trafficking victims" (<https://www.law.umich.edu/clinical/HuTrafficCases/Pages/searchdatabase.aspx>).

On the risk assessments side (one of my other passions — I guess you can have more than one — HT tugs at the heart strings while the risk assessment scenario is realistic), HT should be recognized as high-risk and increasing (unfortunately). This may result in a change in management perspective or a change in your monitoring process. However, the problem with HT is that from the banker's perspective, it does not stand out in the way other higher dollar transactions or structuring may, but unusual activity may be present that you should report. Law enforcement may have the other piece of the puzzle and be able to link your tip or Suspicious Activity Report (SAR) with others to help an investigation. Put keywords, names of URLs, business names, etc., in your search engine that are indicative of HT and run the list frequently to point to issues that may be indicative of potential trafficking. Look for common address scenarios, look at your accounts that have large cash in/out and your due diligence shows no source of income — research, ask, etc. If nothing arises, keep it

on your radar, something may pop up. As has been previously stated, train your staff and take their incident reports seriously. That gut feeling that they or you have, may be just what law enforcement needs to take a case to the next level. Discuss issues and indicators with law enforcement in your area. They trust our instincts and this relationship is very important. It is a collaborative effort. Keep in mind that the overall goal is to decrease HT in the sex and labor arenas.

I recently had the joy of seeing the play *If/Then* in Washington D.C. and the If/Then scenarios came into my thoughts in regards to HT (although that is not what the play is about). *If* the kidnapping, running away, choice to go to the United States to have a better life, and so on, that lead to my being sexually or labor trafficked had not happened, *then* I could have graduated from high school, could have had my Dad walk me down the aisle, could have had a good home and kids. What if HT forever changes the lives of the trafficked persons, if saved; however, many are not. None of it bodes to the good. Even if you play a small part, get involved. *If* you or your staff understand and report potential HT activity, *then* we may stop this blight of HT — at least a little.

Find your passion...

Human trafficking education is one of my passions. This year, I challenged my staff to find their passion. They all reported back to me to present their issues at the regular department meeting and I am pleased that topics such as elder abuse, Internet gambling, local law enforcement issues, identity theft and identity fraud, HT, remote deposit capture issues, money laundering placement, etc., were all claimed and I have found their passion to help them help others through their knowledge. By doing this, their buy-in and excitement about their chosen 'passion' has proven to be an impetus to understand the concerns we all face. Their excitement infects all of us and helps us learn and hone in on unusual activities and the reasons for them. Lead and others will follow — willingly and thrive on it. *What is your passion?* 

Anna Rentschler, CAMS, vice president and BSA officer, Central Bancompany, Jefferson City, MO, USA, anna_rentschler@central-bank.net

¹ Joint testimony of Alice Hill Chair, Blue Campaign U.S. Department of Homeland Security & James Dinkins Executive Associate Director Homeland Security Investigations Immigration and Customs Enforcement U.S. Department of Homeland Security before the Committee on Homeland Security & Governmental Affairs United States Senate "Combating Human Trafficking: Federal, State, and Local Perspectives" on Monday, September 23, 2013



Suzanne Williams: Never stop learning

Suzanne Williams is the assistant director for Corporate Governance in the Bank Supervision and Regulation Division of the Board of Governors of the Federal Reserve System. She is an officer with responsibility for a range of work, including policy, guidance, and supervisory strategies related to the Bank Secrecy Act (BSA), anti-money laundering (AML), Incentive Compensation, and Corporate Governance. Prior to assuming this position, Williams served as manager of the BSA/AML section. She joined the board in 2005 after spending 15 years at the Federal Deposit Insurance Corporation and the Department of the Treasury in various bank supervisory positions. Williams has a master's degree in financial management from University of Maryland and a bachelor's degree in international business from King's College.

ACAMS Today: How did you get into the AML field and can you tell us a little bit about your background?

Suzanne Williams: I started in 1990 as an assistant examiner with the FDIC in the New York region. At that time we were still dealing with the ramifications of the savings and loan crisis and I was working on the exams for many banks that were in a troubled condition. This was an interesting start to my government career in banking supervision because of the banking crisis. As a safety and soundness examiner, I conducted some BSA/AML reviews and also was involved in a loan fraud situation that involved insiders, losses for the bank, an enforcement action and related criminal charges. I enjoyed being a field examiner — analyzing the situation, getting to the heart of the matter.

Later, I took a position at the FDIC's headquarters in Washington D.C. and worked in the international branch on various supervisory and policy issues. In particular, my work that related to the offshore banking centers often involved BSA/AML issues, as well. For example, at that time there was an offshore investment fraud involving banks in Grenada that generated a lot of calls and questions from consumers and others.

These experiences confirmed my interest in AML and were part of what led me to take a position with FinCEN soon after the USA PATRIOT Act had been passed. Since then, I have worked primarily in the AML field and in 2005 I joined the Board of Governors of the Federal Reserve. On a personal note, one of my sisters was at the World Trade Center on 9/11 and we went the whole day without knowing if she was okay. It turned out that she was safe, but this experience brought home to me the importance of AML/CFT work.

AT: Can you give us an insight into the work you do for the Federal Reserve?

SW: I find the work I do for the Federal Reserve quite interesting and challenging. Our group is involved in supervisory, bank specific matters such as enforcement actions related to BSA issues or OFAC sanctions. We are also involved in developing BSA/AML policy and working with international groups on AML issues. It is an interesting mix of topics and subjects and I get to work with a lot of smart, dedicated professionals.

AT: What has been the key to your success in this ever-evolving industry?

SW: In my opinion, the key component is to never stop learning. This may be in a formal or informal context such as on the job. One of the aspects of my job that appeals to me is that there is not a week that goes by that I don't stop and say, "I didn't know that or that is new." There is what you need to know to do the job that is in front of you, but it is also important to ask questions and to have a degree of intellectual curiosity. It helps to understand how the work you do fits into the broader picture for AML compliance or how the bank operates. For example, in my early years as an examiner I realized the importance of talking to a variety of people to make sure you are getting the full picture and that you have your facts correct before reaching a final conclusion or assessment.

AT: There are many facets to compliance, what would you say is your favorite part of working in the AML industry?

SW: My favorite part is that it is really important work about compelling issues. It is interesting because even when you have the same regulatory framework, you have new issues that arise in the environment that you have to interpret and apply the existing rules.

AT: How has the compliance industry changed since you first started working in the field?

SW: The financial industry has gotten more complex and so has the compliance industry. During that time, the USA PATRIOT Act added more provisions and regulations. Twenty years ago, much of the focus for BSA compliance was on CTRs and now there is more emphasis on suspicious activity monitoring, reporting and managing the whole SAR process. There are more international




Treasury's AML Task Force, created in 2012, which includes representatives from DOJ, OFAC, FinCEN, the federal banking agencies, the SEC and the CFTC.

In my opinion, industry outreach is a key component of partnerships. With the various changes in the environment such as new products and delivery methods, it is even more important to have partnerships and open discussions to inform policies. Another important partnership is working with law enforcement. Everyone's efforts are critical in the fight against financial crime and money laundering. The reality is no one group can do it alone and we require each group's perspective and initiatives. Working in partnership is the only way we will all be successful.

AT: You mentioned industry outreach as a key component to partnerships; does the Federal Reserve have its own outreach program?

SW: Yes, we have a program called *Ask the Fed*, which is a free program covering financial and regulatory developments for banking officials. It is run out of our St. Louis Federal Reserve Bank. Last year we had a session where I presented along with other colleagues and we discussed current BSA and OFAC issues. We had over 1,000 people sign up for this session and received positive feedback. In addition, Federal Reserve staff participates in many different speaking engagements and outreach events throughout the year.

AT: How have mentors helped you in your career and what advice do you have for those entering the AML field?

SW: Mentors have helped me by encouraging me to create and take opportunities in order to continue to learn and grow professionally. My advice is to seek out professional and educational opportunities that interest you and add to your skill set, whether it is getting an advanced degree or certification, attending conferences and training sessions, or taking a temporary assignment in another area. You can think of what we do in compliance as information sharing, so it is important to pass along your knowledge and experience with others. 

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

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

aspects and expectations around foreign activity, such as correspondent banking, that you did not have 20 years ago.

AT: Can you share any challenges you encountered in your contributions to AML and how you overcame them for the betterment of the industry?

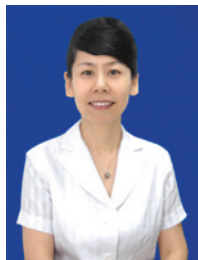
SW: In my opinion, there has sometimes been a tendency to regard compliance as an "add on" exercise rather than an integral part of the bank's operations. I have had people tell me that no bank has ever failed because of AML or BSA, so how important can it be? One of the challenges that we all face in both the private and public sectors is communicating the importance of AML compliance.

Another challenge is that there are a lot of stakeholders both in the public and private sectors for BSA/AML issues. Each stakeholder may have different perspectives, missions and policy objectives. I can't think of another area of supervision that has so

many stakeholders. As a result, there might be times where you think that you have the answer but there are other perspectives and equities that need to be considered. You need to communicate and share ideas to come up with solutions that will satisfy everyone.

AT: Partnerships are extremely important in this industry, what steps have you taken to build and foster key partnerships?

SW: In the public sector we have quite a few partnerships in the form of groups that meet on a regular basis. We are a member of the Treasury-led BSA Advisory Group, which includes representatives of regulatory agencies, law enforcement, and the financial services industry, which covers all aspects of the BSA. The Federal Reserve participates in the FFIEC BSA/AML working group to discuss BSA policy and regulatory matters. In addition to the FFIEC agencies, it includes staff from FinCEN, the SEC, the CFTC, the IRS and OFAC. We also participate in the U.S.



HE Ying:

The importance of knowledge and practice

Ms. HE Ying, Ph.D., is a professor and vice president of Shanghai Finance University, deputy secretary general of the Shanghai Finance Society, and vice chairman of Shanghai Pudong International Finance Institute. Previously, she was vice president of Shanghai Finance College. Vice President HE's major research area is International Finance.

ACAMS Today: What motivated you to lead the effort to establish the bachelor degree in compliance and AML at Shanghai Finance University (SFU) in partnership with ACAMS?

HE Ying: Money laundering is harmful to the society. Not only does money laundering destroy the security of the financial system and the reputation of financial institutions, but it also tremendously perturbs the economic order and social stability of a country. In recent years, money laundering in China has become a prominent issue for this reason crimes of smuggling, drug trafficking, corruption and bribery arose constantly, activities of transferring illicit money abounded in the country. However, the fact is that some officials in financial institutions have insufficient awareness of how important anti-money laundering is, and staff's also have low vigilance to this issue. There is nearly no anti-money laundering education and training in our society, thus experienced professionals on anti-money laundering are in short supply. All above impels us to establish and develop the fundamentals of anti-money laundering. Since SFU was subject

to the administration of the Central Bank of China, we have the responsibility and duty to educate and train the professionals on anti-money laundering. ACAMS is an internationally recognized organization, which has a group of disciplined professionals who are experienced in anti-money laundering, both in knowledge and in practice. It is a perfect collaboration match between the two parties.

AT: What is your vision for this program and its contribution to both SFU and China?

HY: Our vision is to train anti-money laundering professionals both in knowledge and on practice.

AT: How do you view this program's role in the development of AML in China?

HY: Confronted with the severe momentum of anti-money laundering, China lacks the corresponding social fundamentals as well as professional knowledge. The program for the bachelor's degree of compliance and AML will instruct and teach the public about anti-money laundering, strengthen the public cooperation on anti-money laundering activities, and enhance the awareness of individual's legitimate rights and protect their interests. In the meantime, prospective financial practitioners will acquire the skills and methods of anti-money laundering, thus preventing money laundering activities from wide-spreading. Thereby, from the long-term perspective, we could make contributions to anti-money laundering worldwide.

AT: What is the expected impact of this program on the development of practical AML knowledge and building capacity in China?

HY: Universities bear the functions of talent training, scientific research and social service. We hope, through this program, we can train prospective professionals on anti-money laundering, convene a group of experienced anti-money laundering experts to extend the research frontier, and pool the science and technology power of anti-money laundering technology development to provide technical support to the public.

AT: On a personal basis, why did you choose to do the CAMS program?

HY: As a financial practitioner in the past and a financial educator today, I have truly realized the importance of financial security and financial stability. CAMS is my choice to acquire the knowledge on anti-money laundering, and I will be well devoted to anti-money laundering promotion, education and research.

AT: What advice would you have for those interested in entering the AML compliance field?

HY: One should be a person of virtue in personality, profession and dedication. **A**

Interviewed by: Hue Dang, CAMS, head of Asia, ACAMS, Hong Kong, China, hdang@acams.org

贺瑛

贺瑛，女，汉族，1963年3月出生，祖籍浙江省宁波市，中共党员，经济学博士，教授，上海市教学名师。曾任上海金融高等专科学校副校长，现任上海金融学院副院长，分管教学（含体育教学）、实验与现代教育技术、国际交流与合作、招生与毕业生就业、图书馆工作、语言文字工作，协管高教研究工作，联系国际金融学院、中丹学院、国际交流学院、创新创业学院。

曾任中国保险学会理事，现任上海金融学会副秘书长，上海浦东国际金融学会副会长等职。曾获中国人民银行优秀教师、中国金融教育发展基金会优秀教师“金晨奖”、宝钢优秀教师奖、上海市“育才奖”、上海市高校优秀青年教师、上海市新长征突击手、上海市优秀教育工作者等省部级以上荣誉称号。

洗钱行为具有严重的社会危害性，它不仅损害了金融体系的安全和金融机构的信誉，而且对一国正常的经济秩序和社会稳定，具有极大地破坏作用。近年来，随着走私、贩毒、贪污、贿赂等犯罪不断发生，非法转移资金活动大量存在，中国的洗钱问题日渐突出。但一些金融机构特别是领导对反洗钱的重要性认识不足，员工反洗钱意识和警惕性不高，社会反洗钱教育和培训尚处于空白，缺乏一大批有经验的反洗钱专业人士，建立健全反洗钱的各项基础性工作刻不容缓。作为曾经的央行的直属院校，我们有责任，也有义务培养和培训反洗钱专业人士。ACAMS是国际公认的反洗钱专业组织，该组织具有一大批训练有素的专业人士，具有丰富的反洗钱专业知识，两家合作可谓珠联璧合。

培养一批既懂理论，又懂实务的反洗钱专业人士是我们的使命。

面对严峻的反洗钱形势，中国既缺乏反洗钱的社会基础，更缺乏反洗钱的专业知识。该项目的举办，有利于向社会公众普及反洗钱知识，强化社会公众配合反洗钱工作、保护自身合法权益的意识。同时有利于未来金融从业人员掌握反洗钱技能与方法，防范洗钱行为的泛滥。从而为全球的反洗钱工作做出我们应有的贡献。

高等学校具有人才培养、科学研究。通过该项目，不仅要培养一批未来反洗钱专业工作者，同时我们希望通过该项目凝聚一批从事反洗钱研究的专家队伍，共同进行反洗钱学术前沿研究，我们还希望通过该项目汇集一批从事反洗钱技术开发的科技力量，为全社会反洗钱工作提供技术上的支持。

作为曾经的金融从业人员，现在的金融教育工作者，我深感金融安全、金融稳定的重要性。为充实自己的反洗钱知识，以便更好的进行反洗钱宣传、教育、研究，CAMS是我必然的选择。

必须具有高尚的品德、完善的人格、专业的素养、敬业的精神。■



You can play a critical role in our nation's national security

As a professional in the financial industry, you have the ability to play a key role in our nation's national security. The movies show terrorists, criminals and spies in high-speed chases in dark and dangerous places. However, nearly every one of their actions requires money. And, that's where you come in. By being aware of the threats and techniques or those who wish to do us harm, you can serve as a sentinel and patriot and assist in identifying the flow of funds to terrorists and criminal organizations.

I have the great honor of leading the FBI's Terrorist Financing Operations Section (TFOS). On a daily basis the FBI leads law enforcement and domestic intelligence agencies to defeat terrorism through the application of financial investigative techniques and the exploitation of financial intelligence. TFOS analyzes trends to mitigate potential terrorist threats, to identify unknown U.S.-based terrorist cells, and to coordinate the activities of major terrorist financing (TF) cases across the FBI. Furthermore, we investigate persons raising money and conduct forensic reviews of attacks believed to be perpetrated by terrorists to track historical and real-time financial transactions.

We are not able to do our job and be successful without professionals like you who identify and report suspicious activity and trends. The FBI and our law enforcement and intelligence community partners rely on your expertise to unravel the complex nature of financial schemes designed to evade detection. As you are well aware, money laundering is the process of concealing sources of money raised by criminal activity; whereas TF is defined by how its funds are used, for example, paying for the travel or training of individual(s) to commit a terrorist act; purchasing components of an explosive device; false identification; ammunition or payments to terrorists' families.

To further complicate matters, often small sums of money finance major attacks. While you can never put a price on the loss of life and the human suffering of families and friends of victims, the cost of terror attacks is nominal.

One of our most important tools is the financial industry and professionals like you who take the time to learn about the threats and the indicators of terrorism and related financing.

Possible indicators of terrorist financing include:

- Account transfers by non-government organizations (NGOs), charities, etc., to financial entities in countries known to be tax havens, areas of political conflict or non-cooperative with the Financial Action Task Force (FATF) on money laundering.
- Using multiple accounts under the same personal or business name to collect and transfer funds to the same foreign beneficiaries.
- Repeated cash withdrawals in high-risk regions.
- Suspicious activity within charities/NGOs established to support areas in high-risk or conflict regions.
- A high volume of incoming and outgoing wire transfers for no logical reason or economic purpose coming from, going to or transiting through FATF non-cooperative and sympathizer nations.
- A large number of cash deposits in the U.S. with corresponding withdrawals in countries of concern, or non-cooperative with FATF. Large cash withdrawals, whether in one lump sum or in a series of smaller transactions, may be moved outside the formal banking system and hand-carried to individuals or groups involved in TF.

What are some examples of reactive and proactive threat management? How can we use financial intelligence to move TF investigations forward?

Much of the investigative work in TF cases is reactive. For example, let's evaluate a \$200,000 wire transfer from a U.S. bank to a money services business (MSB) in a TF country of interest (COI). Review of that transaction on a bank statement provided the name of another person potentially involved in a major terrorist attack overseas. The FBI then identified this individual, found associated phone numbers and engaged its partners to analyze bulk phone activity between this individual and potential TF subjects overseas. FBI analysis of the phone and financials records led to identifying additional TF associates, whom we then worked with our financial partners to research related suspicious activity and build preliminary investigations in additional field offices. Without this financial transaction, the additional associates would not have been identified.

In a previously adjudicated case called Operation Smokescreen, a joint investigation involving over a dozen local, state and federal investigative agencies, a Hezbollah cell operating out of Charlotte, North Carolina bought mass quantities of cigarettes in cash from local wholesalers and resold them in states with much higher sales and tax bases on cigarettes. While surveillance and other traditional law enforcement investigative techniques identified individuals involved in the operation, forensic accounting results of Smokescreen revealed over \$8 million funneled through more than 500 banks accounts. Investigative partners within several U.S. banks assisted law enforcement in not only identifying suspicious financial transactions, but account statements disclosed the purchase of global positioning systems, night vision goggles, laser range finders, stun guns, handheld

radios and receivers, among other tactical equipment being sent to the Middle East to Hezbollah. Members of the cell were convicted on material support to designated foreign terrorist organizations, in addition to long-established criminal charges for credit card, immigration and bank fraud alongside identity theft, tax evasion and money laundering. Again, financial records were crucial to the terrorism investigation.

In addition to traditional reactive financial investigations, our goal is to proactively identify potential TF activity before an attack occurs and innocent lives are lost. TFOS works with financial institutions to provide targeting indicators so bank investigators have the information they need to identify non-traditional suspicious financial activity. By example, indicators may include accounts opened within the U.S., with a pattern of cash withdrawals in high-risk countries. This collaboration enhances the financial institutions' due diligence procedures while assisting law enforcement, and may include financial institutions providing data on potential TF subjects previously unknown to the FBI.

What's going on in Syria and why is it important to the average U.S. citizen?

The civil war in Syria is a security issue for its neighbors in Lebanon, Jordan, Iraq, Israel, with the potential to impact Europe and the

U.S. During recent congressional testimony the Director of National Intelligence, James Clapper told the Senate Intelligence Committee that such al-Qaeda groups in Syria have started training camps "to train people to go back to their countries" — one of the newest threats emerging in the past year to U.S. security. He said "al-Nusra Front, to name one ... does have aspirations for attacks on the homeland." In addition, in countries within the region, such as Kuwait, U.S. think tanks studying TF activity have reported charities and individuals channeling money to a myriad of Syria's rebel groups. Money is flowing to Syria from the U.S. to fund the various terrorist groups; we need your assistance in stopping those funds.

In sum, thousands of innocent lives have been lost due to money and materials getting to extremists and terrorists before we could stop the flow. While there are donors within the Middle East and other parts of the world funding different groups fighting the civil war, collection of funds may be happening on our own soil. Therefore, it's important for us to work together to identify and research the previously-mentioned suspicious financial activities above, and to collaborate the investigation of other resourceful techniques used to collect U.S. dollars for TF activities in Syria and beyond.

How you can contribute

I encourage each of you to research the international conflicts and threats facing our world and apply that knowledge to your financial reporting expertise. By combining your knowledge of the threat and financial compliance, you can serve your country and assist in protecting the financial industry from unwittingly supporting terrorism or other illicit activity. Protecting our country is everyone's job.

Financial institutions should utilize FinCEN tools for information sharing and reporting (314a and 314b) options.


Financial institutions may contact their local FBI office's Joint Terrorism Task Force and request training and participation in a banking working group.

Financial institutions should contact TFOS: at 202-324-5914 for information on specific collection parameters related to Syria, Yemen, Afghanistan, Somalia and other high-threat regions.

Resources materials

- West Point Counterterrorism Center publishes excellent materials on threats by groups and regions: <http://www.ctc.usma.edu/>
- Office of the Director of National Intelligence: <http://www.dni.gov/index.php>
- U.S. Department of Treasury — Illicit Financing and Terrorism: <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/default.aspx>

Conclusion

Thank you for your time and interest in protecting our nation's security. Working together, we can use financial intelligence to assist in detecting and defeating terrorism. The threat is too large for the FBI to handle alone, so we rely on our partners in the financial industry, federal, state and local law enforcement, intelligence community and foreign partners to succeed. 

Jane Rhodes-Wolfe, section chief, Terrorism Financing Operations Section (TFOS), FBI, USA, Jane.Rhodes-Wolfe@ic.fbi.gov



*“Connecting the **dots**”*



Connecting the dots were the opening comments and theme for the presentation given by Joy Smith, MP, Government of Canada at the Together Let's Stop Traffick Summit last October in Ottawa, Canada.

The Summit was a collaborative, international three-day working conference, FBI National Academy Associates (FBINAA) Charitable Foundation initiative produced and hosted by the International Police Training Institute (IPTI). The weekend represented the first phase of a four pronged program to build the world's first International Resource and Coordination Centre (IRCC). Information will be fed 24/7 from every corner of the globe, cross-referencing criminal shipments, trafficking patterns and reported disappearances in a concerted effort to close the loop on organized crime crossing national and international borders. The views, expertise and experiences of delegates were actively sought. The 100 plus attendees included law enforcement, border agencies, non-government organizations (NGOs), transportation, logistics and victim support and one anti-money laundering (AML) banking compliance officer.

The first day and a half we heard multiple presenters from a wide range of involvement in human trafficking (HT) representing a global footprint. Each speaker drew from their professional and/or personal experiences. This allowed attendees to increase their knowledge of this global crime and also to fuel the passion to eradicate all forms of HT.

Timea Eva Nagy shared her survivor story of being a victim to the promise of a well-paying job in Canada from her home country of Hungary. Her story is a reminder that human trafficking knows no boundaries or is limited by social class. Her mother was a police officer, and Nagy was established in journalism and communications. In 1998, she fell on hard times and answered an ad for summer employment as a nanny in a Hungarian speaking community in Canada. However, when she arrived in Canada, there was no nanny position, and she became a victim to the sex industry. She was able to escape after three and a half months.

In 2009, she founded Walk With Me, and became an advocate for victims of HT. Based in Toronto, Nagy works closely with the Royal Canadian Mounted Police (RCMP) and legislators to give aid to survivors and rescue victims.

Jamie McIntosh, founder and former executive director of International Justice Mission (IJM) Canada and Mark Clookie, global vice president of investigations and law enforcement at IJM, U.S., highlighted undercover investigative efforts in twelve countries, and their goal to disrupt and dismantle the criminal enterprises. Leif Coorlim, editorial director, CNN Freedom Project, showed segments from his video production *Freedom Project*. The power of the media is evident in that production of an estimated 400 stories and 7,080 NGOs. Look for continuing additions at: www.thecnn-freedomproject.blogs.cnn.com.

Human trafficking
knows no boundaries
or is limited by
social class

The U.S. Department of Homeland Security and the Blue Campaign was represented by Maria Odom, CIS ombudsman and Blue Campaign chair and Scott Santoro, The Blue Campaign training advisor. Odom's presentation reminded us that trafficking includes domestic servitude and she shared riveting examples from the Washington D.C. area. Santoro has a refreshing approach to training with the multiple facets of this subject. He scripts various scenarios and produces a video. The training audience is then asked to

identify evidence or clues that the situation could be a trafficking situation. A much more engaging and memorable training experience than a computer-based multiple choice quiz following case studies.

Jennifer Kimball, systems and data coordinator from Polaris Project shared information collected the last five years on sex and labor trafficking. I appreciated her visual graphs and heat maps! She also shared how text messaging to the national hotline is a new channel to both help victims and identify patterns in HT to prevent it in the future. Read more on their success and data analytics at their web site: www.polaris-project.org.

Adobe Senior Solutions Architect John Penn II dedicates his work to help law enforcement solve cases with the use of digital imagery. His career focus was sparked by a law enforcement conference several years ago and a session presented by the National Center for Missing and Exploited Children (NCMEC). Penn was able to direct his intrigue on how imagery could be used to rescue child victims into a full-time job and focus within Adobe. Due to Penn's efforts, Adobe created the title of Senior Solutions Architect for Law Enforcement Technologies. Congratulations John!

NCMEC's President and CEO Ernie Allen opened discussion on the explosion of child pornography, the movement of HT to the Internet and the challenges of anonymous virtual currencies. In addition, he gave testimony to the U.S. Senate this last November titled "Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies." Allen is enthusiastic about the potential with virtual currencies and the digital economy, but concerned with the criminal enterprises that are moving their activity to this unregulated unbanked digital global economy. Follow what NCMEC is doing by adding their webpage to your favorites: www.missingkids.com.

"No one can do everything, but everyone can do something" was the challenge George Mueller, assistant chief Los Angeles County DA's Office, gave attendees. He shared trends of gangs swapping girls, girls being recruited on Facebook and Twitter and case studies

of trafficking in airports and truckstops. His challenge to the group was defined by asking us to educate ourselves, know our neighbors, serve our communities, listen and learn, know how to act and to be aware of the law.

No one can do
everything, but
everyone can do
something

Attendees were encouraged to "think outside the box and don't be quiet" by Virginia Sundbury, human trafficking lawyer, as she shared her story of a sweatshop in paradise in American Samoa. Andy Desmond, an expert in Nigerian organized trafficking, added to the global perspective. His recent focus is with a specific geographic area of Nigeria and the use of witchcraft to control the victims trafficked into London and internationally. His presentation provided case studies and a form of manipulation that many of us were not aware existed.

During our Summit, Project Spade, a massive international child pornography bust reported 348 arrests and at least 386 children rescued from sexual exploitation. We were able to hear some of the details firsthand from William Blair, Toronto chief of police, and Todd Shean, assistant commissioner, federal policing support services RCMP. Joy Smith, MP Government of Canada, congratulated the extensive teams and extended efforts of the more than 50 countries that contributed to the investigation. This is a prime example of how collaborative efforts can connect the dots and result in successful arrests, rescue and aftercare for the victims.

The balance of the weekend was spent defining specific goals for the creation of the International Resource and Coordination Centre and forming working groups to accomplish the items on the task list. Collectively as a group, we created several hundred topics to address. After those were identified, we defined descriptions, current situations, future state, move to action and opportunities for action. One of the prevalent statements made for the weekend, was how well everyone worked together and left personal agendas and egos at the door. We exceeded the anticipated goals with the collaborative efforts of the working groups. The list of opportunities for action remains long, and is fluid as knowledge, technology, current events and contributors impact the project.

On behalf of "Together Let's Stop Traffick" I want to extend an invitation to you to visit the web site: www.togetherletsstoptraffick.org. We are planning webinars that will be available to everyone. The 2014 Summit is in early planning stages with a location and date to be announced soon. Watch the web site for updates and announcements or become part of the LinkedIn community. Consider bringing your "dots" to connect virtually or by attending the Summit this fall!

The ACAMS community is passionate about eradicating this global crime. How do we identify where our "dots" are to connect? What will it look like if all the dots from every sector connected and fabricated a global net against human trafficking?

Last year I made it a personal goal to raise awareness within my community and step up my involvement to a higher level. Both of those goals were accomplished, but what surprised me, was how my awareness expanded! I am humbled and excited with the efforts and successes of others in tackling this horrific crime.

I would like to again share the challenge of my new friend George Mueller, "No one can do everything, but everyone can do something!" 

Sande Bayer, CAMS, GTC chapter board member, vice president AML Compliance, U.S. Bank, Minneapolis, MN, USA

PATRIOT OFFICER®

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

Endorsed By The Largest Bankers Associations and Has Passed Examinations

“THOUSANDS OF TIMES”

Financial
Intelligence
Center



Compliance
Network
UCEN.net



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

Barbara Keller, CAMS: AML—the mansion industry



A *CAMS Today* had the opportunity to speak with Barbara Keller, CAMS who recently retired from Federal service, where she worked at the GAO and ended her Federal career at FinCEN.

Barbara I. Keller retired from Federal service in August 2013 and is now an independent consultant and an advisor with Treasury's Office of Technical Assistance. Most recently she co-led a workshop on the development of Financial Intelligence Units for the Financial Services Volunteer Corps in Tanzania. She spent the last four years of her federal career as the deputy associate director for compliance and enforcement at the Financial Crimes Enforcement Network (FinCEN), where she oversaw the activities of the compliance and enforcement offices. In this role, she worked to better ensure industry compliance with the Bank Secrecy Act (BSA) through supporting, overseeing, and working in partnership with the federal and state agencies and organizations directly examining financial institutions for BSA compliance and, through enforcement, sought to sanction egregious violations of the BSA, obtain corrective action, and deter future non-compliance. Keller also worked with law enforcement and the financial industry to improve BSA compliance among financial institutions.

Keller joined FinCEN in September 2009 after 26 years with the U.S. Government Accountability Office (GAO). She began her career in Washington, D.C. then spent two years in GAO's office in Frankfurt, Germany where she worked on military and foreign assistance assignments in Europe and Africa. Back in Washington, before moving into the financial markets area, Keller spent seven years as the analyst-in-charge of assignments on a number of international trade and competitiveness issues. For the last 10 years of her GAO career, Keller was an assistant director with the Financial Markets and Community Investment team. In this position she managed a number of assignments on financial market topics mostly dealing with

anti-money laundering and various international issues. She led reviews of the effectiveness of BSA compliance and enforcement efforts among government agencies, suspicious activity reporting, currency transaction reporting, USA PATRIOT Act implementation, the vulnerability of the credit card and Internet gambling industries to money laundering, and implementation of the National Money Laundering Strategy.

Keller is a Certified Anti-Money Laundering Specialist. She holds a B.S. in Languages from Georgetown University and an M.A. in Public Administration from the University of Virginia.

ACAMS Today: Can you give us an insight into the work you did for the GAO?

Barbara Keller: Because of its broad mission, GAO is well-positioned to develop a comprehensive picture on whatever program or issue it reviews. Through its work, GAO provides Congress and, ultimately the American people, with objective reports on how the government is doing and ways for it to improve. In the AML area, GAO is the only agency able to look across government and develop a holistic view. As a GAO assistant director in the financial markets area, I led engagements on a number of AML/CFT topics over an eight year period including the effectiveness of BSA compliance and enforcement efforts among government agencies, suspicious activity and currency transaction reporting, USA PATRIOT Act implementation, and the vulnerability of the credit card and Internet gambling industries to money laundering. I also served as the GAO liaison to FinCEN and as an advisor on other GAO engagements that involved FinCEN or other Treasury offices involved in AML/CFT. Over the years, I developed a broad understanding not only of U.S. government AML efforts, but also of how the financial industry worked to comply with AML/CFT regulations. I got to know the work of the financial regulators who oversaw AML compliance as well as the IRS group that examines non-bank financial

institutions. I also got to know the work of the Department of Justice and law enforcement agencies. Plus, I met with industry associations and countless financial institutions to get their perspective.

AT: Can you share any challenges you encountered in your contributions and how you overcame them for the betterment of the industry?

BK: My first GAO AML engagement began in the summer of 2001 when we were asked by the Permanent Subcommittee on Investigations to look into the vulnerability of the credit card industry to money laundering. When we held introductory meetings with bank regulators, bankers associations, and the credit card industry they all looked at us like we were from another planet and downplayed the concern — there were much easier ways to launder money, why go through the trouble of using credit cards? After 9/11 and the passage of the USA PATRIOT Act, views changed. Then in 2004, there was another wake-up call with the penalties against Riggs Bank and the Senate Banking Committee hearing where the bank regulators were told to improve their AML oversight. GAO was then asked to oversee the regulators' efforts. Over the 26 years that I was at GAO, it was always a challenge to convince agencies that we really were "there to help." The beauty of GAO is its ability to see the forest through the trees and develop recommendations that, if implemented, could improve government operations. In the AML area, GAO, as an oversight agency, has the unique position of being able to talk to all sides (regulators, law enforcement, and industry) and provide Congress with an objective assessment of the problems it finds and make recommendations to fix them. What I didn't know until I went to FinCEN was just how hard it could be to implement GAO's recommendations. I got a whole new perspective going from the Legislative to the Executive Branch — from oversight to operations, if you will. I came to FinCEN with a very different experience

than most — I understood the viewpoints of all players in the AML area from an objective, oversight perspective, which enhanced the contributions I could make to the agency's mission.

AT: How has the industry changed since you became involved in it?

BK: AML compliance has only grown in importance in the years since I became involved in it. Although the basics are still the same, there are many more regulations and regulated entities since the USA PATRIOT Act was passed in 2001. Plus, technology has had and continues to have a significant impact on the ability of financial institutions to monitor the activities of their customers and, at the same time, has enabled criminals to find new ways to launder money and commit other financial crimes. Although the civil and criminal penalties have increased since I first started working on AML issues, one thing that remains the same is the reputational risk financial institutions face if they do not take their AML compliance responsibilities seriously.

AT: What is the best piece of advice you received from an AML peer?

BK: I'm not sure this is exactly a piece of advice, but what I thought of when I heard this question was something a GAO colleague said to me about the AML field back in 2008 — "This isn't a cottage industry, it's a McMansion industry!" It has only continued to grow since then so maybe now it qualifies as a "mansion industry." Back in the mid-2000s, I think some in the field thought financial institutions would get into compliance and we would all move on. In fact, it seems to be just the opposite. Although financial institutions now have a better understanding of their AML compliance responsibilities, they are always facing new challenges and need to be vigilant and ensure that they are regularly updating their risk assessments, improving their monitoring tools, and making whatever tweaks to their systems and AML program that are required.

AT: What would you say to anyone who is interested in entering this career path?


BK: My advice to anyone interested in entering the AML field is to think more broadly than just AML in both the qualifications they develop and their job search. We tend to use AML as something of a catch-all

phrase, and many times AML and economic sanctions noncompliance are grouped together, but there are many other types of financial crime that financial institutions need to be on the look-out for. Also, there are intersections between money laundering and fraud and financial institutions are finding value and efficiencies in merging these departments or at least having them work more closely together. Whether you want to work in this field in the private or public sector, there are lots of opportunities and ways to do it.

AT: What are your next steps in the AML field?

BK: Although I retired from FinCEN, after 30 years of government service, I am not leaving the AML field. In fact, I have joined Treasury's Office of Technical Assistance as a contract employee and will be traveling to developing countries to provide technical assistance as part of the Economic Crimes Team. I hope that my unique background in both program evaluation and AML will allow me to accurately assess countries' needs and advise them on how to build their AML/CFT programs and infrastructure. I am also exploring other ways in which I can be active in the field.

AT: What AML book are you currently reading?

BK: I recently listened to the ACAMS webinar with Juan Zarate, former Treasury assistant secretary for terrorist financing and financial crimes and deputy national security advisor for combating terrorism, about his new book, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, and immediately bought it. I had initially met Juan in 2003 when GAO was asked by the House Financial Services Committee to look into the U.S. government's hunt for Saddam Hussein's assets. GAO was, in effect, reviewing Treasury and other U.S. government agencies' actions almost in real-time in their efforts to track down not only Iraqi assets but the assets of other corrupt foreign dictators. That engagement was my introduction to the terrorist financing area. The book is a fascinating account of those early years. Little did I know back in 2003 that I would ultimately finish my Federal career at FinCEN, an agency that has played a significant role in the new era that Juan covers in his book. 

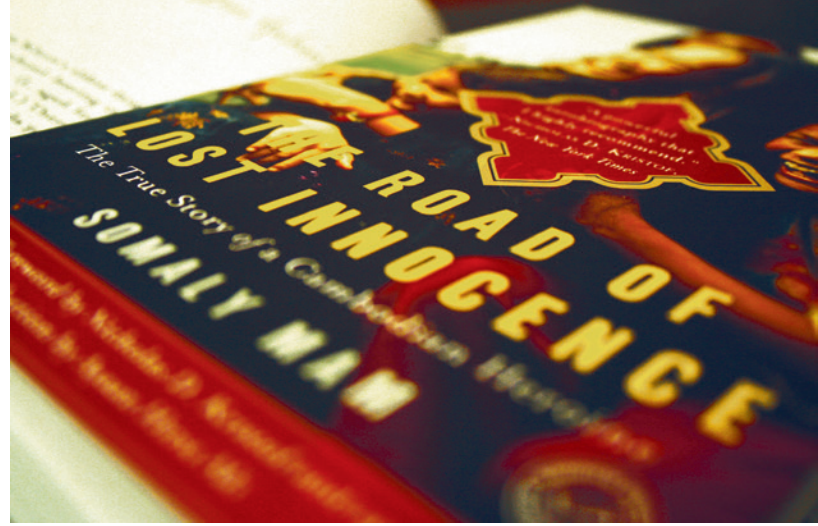
Interviewed by:

Tanya Montoya, product development manager, ACAMS, Miami, FL, USA, tmon-toya@acams.org

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



A modern day heroine and her fight against human trafficking



The Road to Lost Innocence by Somaly Mam with a foreword by Nicholas D. Kristoff and an introduction by Ayaan Hirsi Ali

If there was ever a question as to what human trafficking (HT) is, Somaly Mam gives readers a firsthand account of her life as a HT victim who eventually escaped and found her voice as one of the bravest, most prominent leaders in the fight against HT. Born in 1970 to a life of extreme poverty, Somaly tells the story of how she was sold into sexual slavery at a very young age and forced to work in a brothel with other women and children for many years before she managed to escape and live a new life abroad.

Somaly's story did not end at escape though, it was just the beginning. Before the activist known to us all as Somaly moved to France, she made a promise to herself that she would one day return to help those that stayed behind, and that is what she did. Somaly returned to Cambodia with a new vision: To help as many victims as possible, one by one. Rather than hiding in fear upon her return, Somaly launched rescue missions, secretly set her home up as a shelter for sex trafficking victims and focused a great deal of her work to support the empowerment of victims, so that they too could one day help others. By 1996, Somaly established the Cambodian NGO Acting for Women in Distressing Situations (AFESIP), and through the support of international organizations, she was able to raise enough funds to build a women's shelter, and held its official opening ceremony on March 8, 1997, Women's Day.

Since then, Somaly has continued working tirelessly with law enforcement and organizations around the globe, including the United Nations. The awards are endless: One of TIME magazine's 100 Most Influential People in 2009, A CNN hero 2011, CNN Freedom Project, Fortune Magazine's Most Powerful Women and Fast Company's League of Extraordinary Women. Somaly

has also won numerous accolades from the U.S. Department of Homeland Security and her work has been recognized by the U.S. Department of State.

Now as president of the Somaly Mam Foundation in the U.S., Somaly continues the fight not just here but also in Cambodia, even after she and her family have received several death threats and have themselves been victims of violence.

How can AML officials help in the fight against HT? According to the Somaly Mam Foundation, over two million women and children are sold into sexual slavery each year and endless number of criminals are profiting from the multi-billion dollar HT industry. Somaly teaches us that "silence" is a recurring theme that permeates these victims' lives, and as leaders in the AML and financial crimes prevention space, it is imperative that we begin to explain to senior management how financial institutions can have a positive effect on stopping this horrific crime.

Recently at ACAMS 12th Annual AML & Financial Crime Conference, Supervisory Special Agent David Rogers spoke passionately during the HT session as he explained the victim-centered approach, which focuses on rescuing and restoring victims first and foremost. This new approach of educating law enforcement agents, and those in the financial sector to place victims as the priority, teaches us that humanizing this crime and understanding the victim's perspective is just as important as following the money trail during the investigative process. You may also ask, "Why is it a challenge to shift the focus to the sex buyers and perpetrators?" The answer lies in the fact that there are two requirements that must be met before law enforcement is able to prosecute: 1) Law enforcement must prove that

the intent was intentionally a commercial sex transaction, 2) Unless the victim is under 18, law enforcement must also prove that it is a known commercial sex transaction brought about through force, fraud or coercion. Somaly wrote this book for the very reason Rogers works in favor of the victim-centered approach; as said by Somaly herself, "On their behalf, I would like this book to serve as a call to the governments of the world to get involved in the battle against the sexual exploitation of women and children. Victims are victims in every country."

After reading this memoir, I am left with the notion that just as Somaly found the strength to not just survive but thrive in spite of her "road of lost innocence," we as AML professionals and civilians also have the power and the obligation to join the fight against this horrific crime: Even if it is "One prosecution at a time, one victim at a time, one awareness campaign at a time."

To learn more visit: <http://www.acams.org/topics/human-trafficking/>

Somaly Mam Foundation — www.somaly.org

Polaris Project — www.polarisproject.org

A Global Report on Trafficking in Persons (United Nations Office on Drugs and Crime) www.unodc.org

Office to Monitor and Combat Trafficking in Persons (US Department of State)

Human Trafficking FBI Initiatives — www.fbi.gov

Blue Campaign — U.S. Department of Homeland Security www.dhs.gov 

Book Review by: Tanya Montoya, product development manager, ACAMS, Miami, FL, USA, tmontoya@acams.org

TODAY I STOP TALKING AND START COMMUNICATING.

It's a noisy,
cluttered,
chaotic world.

CSI Secure Connect offers a proven tool for communicating more effectively throughout your organization. Securely post, collaborate and schedule meetings from workstations, laptops and mobile devices, allowing users to be more productive and connected than ever before.

csiweb.com/saywhat



Women in AML showcase

The spotlight collage is dedicated to showcasing influential women who have been in the AML and financial crime prevention field for many years and also to highlight the newcomers into the field who are making their own mark in this exciting industry.

ACAMS Today asked several veterans in the AML and financial crime prevention field to share their proudest AML career moment and this is what they shared with us...



“When I realized AML compliance had gone mainstream and that the senior most leadership at financial institutions now care about getting AML compliance right.”

—**JENNIFER SHASKY CALVERY**, director, Financial Crimes Enforcement Network (Fincen), United States



“My proudest AML career moment is my participation as a member of the executive committee, in the creation of the ACAMS Montreal chapter because we are the first French speaking ACAMS chapter in the world. It is an opportunity for ACAMS members in Quebec to connect and network face-to-face and it is also a first step to the creation of other French speaking ACAMS chapters around the world.”

—**MARTINE LEROUX**,
CAMS, AML detection
and surveillance
manager, National Bank
of Canada, Canada

WOMEN IN AML



“My proudest AML career moment was being recently appointed as co-chair of the SIFMA AML and Financial Crimes Committee. Having served on the Committee for over 15 years, including serving as its AML Hedge Fund sub-committee chair where I was a primary author of its Hedge Fund Suggested Due Diligence Practices piece (published in 2009), this new appointment was particularly gratifying.”

—**MEG ZUCKER**, global AML officer, United States



“Throughout my AML career, I have experienced a lot of satisfying moments, such as being invited as an expert to EAG, guiding banks’ efforts in remediation of AML deficiencies as their compliance officer, and becoming a trusted advisor to a number of financial institutions at FIS-EGRC. I am particularly proud that the advice that I provide to my clients not only helps them stay compliant with the regulations, but also eventually closes (or at least narrows) the possibilities for criminal elements to execute money laundering through our financial system.”

—**ZOYA FAYNLEYB**, CAMS, senior manager, AML/sanctions at FIS EGRC, United States



“My proudest AML career moment was working with a team to remove my country’s name from FATF blacklist. The defining moment was when the Financial Intelligence Unit of The Bahamas, was declared compliant with FATF Recommendation 26—fulfilling.”

—**SHARMIE FARRINGTON AUSTIN**, data protection commissioner, Ministry of Finance, Bahamas

“My proudest AML career moment came when my very first client invited me to service them a second time. I knew then that I was adding value. I have since become their ‘go to’ for any and all AML compliance matters.”

—**LAURA H. GOLDZUNG**, CFE, CAMS, AML Audit Services, LLC, United States



WOMEN IN AML



“When I was the State Department’s Director of Counterterrorism Finance Programs, my team received an “A–” grade from the 9/11 Commission (the highest grade it granted) in 2005 for our efforts to following the money trail and combat terrorist financing and money laundering.”

—**CELINA REALUYO**, president CBR Global Advisors, LLC, professor of practice, National Defense University, United States

“As a BSA compliance officer my proudest career moment cannot be measured by a single item or gesture. My CAMS association has afforded me the direct opportunity to service clients on all levels of compliance making a difference in the day-to-day activities and lives of my clients and giving me a true sense of worth in the duties I perform.”

—**CATHY SCHARF**, CAMS, vice president and operations officer, United States



“My proudest AML career moment is chasing our former President Chen’s dirty money trail in Switzerland and Singapore in autumn of 2008. The money laundering investigation was ignited from freezing a suspicious bank account in Switzerland. I evaluated the possibilities and results of opening an abroad investigation and then made a brave decision, which made our prosecutors start a global chasing of President Chen’s proceeds of crime. The chasing of Chen’s dirty money turned out to be Taiwan’s scandal of the century.”

—**JOANNA CHI-JEN CHING**, CAMS, head prosecutor, Taiwan High Prosecutors Office, Taiwan



“I would have to say my proudest moments have been developing efficiencies in our BSA program with our AML software. I work closely with the software to validate all transaction activity and have created process and reporting that help us to effectively identify suspicious activity. The processes have been validated effective through audits and exams from external and regulatory auditors. We have repeatedly received exams with little to no findings and I accredit a lot of that success to the processes that I have put in place with our software.”

—**PAULA TOBAR**, CAMS, AVP BSA/USA Patriot Act officer, Bank of Nevada, United States



“My proudest AML career moment was when I read that a tax attorney, who was the subject of numerous SAR filings by my Department, pleaded guilty to falsifying tax returns and was sentenced to federal prison. This case highlights the successful collaboration between the financial services industry and law enforcement.”

—**SUSAN WAHBA**, CAMS, EVP and chief risk officer, Grandpoint Bank, United States

WOMEN IN AML



“I am most proud of the partnerships we have formed in the ongoing fight against money laundering. The ability of prosecutors, law enforcement agents, regulators and industry professionals to work together is imperative to our collective success in the ever changing AML environment.”

—**MERYL LUTSKY**, chief, crime proceeds strike force, Criminal Enforcement & Financial Crimes Bureau, United States



“For the last 12 years I have spearheaded a very successful yearly symposium for the Puerto Rico Bankers Association, which has been the primary forum to educate the financial community in AML matters. It has provided our local industry with access to U.S. regulators and help foster an open relation and dialogue with law enforcement for better identification and submission of suspicious activities.”

—**MARÍA DE LOURDES JIMÉNEZ, ESQ.**, senior vice president and division manager, Banco Popular de Puerto Rico, Puerto Rico



“My proudest AML career moment was when *ACAMS Today* published my article “\$5.00 to ruin the life of children and women: Internet ad sites used to launder money in promoting prostitution/human trafficking.” This was my proudest moment because my published article opened the door for me to start lobbying for a FinCEN SAR check box category for human trafficking. Since my article was published, I was able to be printed in the FinCEN 23rd edition of the SAR Activity Review Tips, Trends and Issues with my article titled, “FinCEN SAR check box for Human Trafficking.” I have continued lobbying for the SAR to be changed and I can report back that Congress has commissioned FinCEN to come up with red flag indicators for human trafficking. I was honored to assist with this and had a conference call with FinCEN where we brainstormed the red flag indicators for human trafficking based on my experience. My goal is to help in the fight to end human trafficking by following the illicit money trail through the SAR process to help rescue the victims, save lives and arrest the traffickers and johns.”

—**JOANN ALICEA, CFCI**, certified financial crimes investigator, United States

“Many of my proudest AML career moments were truly team efforts. However, obtaining the CAMS certification was certainly an individual highlight for me. I appreciate all those dedicated AML professionals who encouraged me, and hope I can do the same for others.”

—**MARY BASHORE**, CAMS, president, Bashore Business Solutions, LLC, United States



WOMEN IN AML

“One of my proudest and most challenging AML career moves was establishing a BSA/AML compliance program for a higher risk non-bank financial institution in a business environment where BSA/AML compliance, as a best practice, was met with competing priorities and executive management was resistant to change. Through this experience, I learned the importance of effective communication and the power of influence.”

—**FREDIA S. WYNNE**, CAMS, senior specialty risk examiner, United States



“The date was March 19, 2013, and the location was sunny Hollywood, Florida, the venue for the 18th Annual ACAMS International AML and Financial Crimes Conference. This was the day that ACAMS Executive Vice President John J. Byrne publicly recognized the efforts of the BSA Coalition by giving it the ACAMS Private-Public Sector Service Award. As a regulatory advisor to this unique organization, a group of AML professionals who discuss and resolve BSA/AML issues, I have learned so much. I am honored to be among women recognized in the AML field.”

—**ELAINE RUDOLPH YANCEY**, MBA, CAMS, managing examiner, The Federal Reserve Bank of Richmond, United States



“My moments of greatest job satisfaction have always centered on learning that the information we provide to law enforcement is being used and is of value. It's great to hear that our SARs are ‘very useful.’ As for what I am most proud of, it is my team. Their skills and dedication are incredible. I truly believe that we are only as successful as the teams we build.”

—**DEBBIE HITZEROTH**, CAMS, BSA/OFAC compliance officer, United States Postal Service, United States



“Several proud moments come to mind...earning my CAMS certification, publishing my first article in *ACAMS Today*, and I feel proud each day working for an innovative company that plays a significant role in the fight against money laundering, terrorist financing and other financial crime.”

—**CAROL STABILE**, CAMS, senior business manager, Safe Banking Systems, United States



“My proudest AML career moment was forming the ACAMS Southern California (SoCal) Chapter in 2009. As the founder and co-chair, it has been a rewarding experience to be able to provide Southern California professionals with affordable access to learning events unique to our community and networking opportunities. In addition, the ACAMS SoCal Chapter was recognized as the chapter of the year in 2012. That was an exceptional proud moment, knowing that the hard work and dedication of the SoCal Board was recognized for the efforts and standards we established to carry out our mission.”

—**ELIZABETH A. SLIM**, CAMS, senior vice president, BSA officer, 1st Enterprise Bank, United States





Dig deeper, uncover more

RDC specializes in uncovering hard-to-find information on individuals and organizations in emerging markets and other high-risk economies so that you can safely grow your business without increasing your risk.

The world's leading financial institutions trust RDC for decision-ready risk intelligence and compliance services that truly meet the needs of their worldwide operations. A consistent global approach significantly reduces risk, stands up to regulatory scrutiny and maximizes your compliance resources.

Contact us today to find out how we can enhance your global Anti-Money Laundering and Know Your Customer programs. *Grow Safely, Grow Globally*



Proven Efficiency.
Superior Protection.
Smarter Risk Management.

Learn more about RDC's decision ready intelligence.
email: information@rdc.com | visit: www.rdc.com

Let's talk. Americas (888) 533.1181 | International 44(0)20.7959.2245

Women in AML showcase



“I hope to continue to represent ACAMS here in Canada and in the global arena, in creating training opportunities and communicating changes to the AML environment. Additionally, I hope that by encouraging dialogue and open participation, this will only serve to enrich my own knowledge and experience which in turn I can use to impact the AML program within the Royal Bank of Canada (RBC) and the AML/ATF/Sanctions regulatory environment here in Canada.”

—**ROSALIND LARUCCIA**, CAMS, senior manager, AML audit, Internal Audit Services, Royal Bank of Canada, Canada

ACAMS Today also had the opportunity to chat with the newcomers in the industry and asked them what they hope to achieve in the AML field and here is what they shared with us...



“Strong BSA/AML standards should not be the burden of compliance officers alone. My business counterparts are in the process of getting CAMS certified. I’m dedicated to achieving that level of shared commitment to AML values in the larger banking industry.”

—**RACHELE C. BYRNE**, CAMS, vice president, AML compliance officer at a global financial services company, United States

“Raising awareness around money laundering schemes, particularly in an environment where products and services are evolving so quickly, is important to me. Through education, training and involvement in organizations such as ACAMS we can help deliver to the industry timely information to help organizations and employees stay vigilant.”

—**SEPIDEH BEHRAM**, Esq., United States



WOMEN IN AML



“I hope to continue to support companies in managing the compliance, regulatory and reputational risks attached to their existing and prospective customers, by sharing insights, and offering thought leadership on emerging and shifting risk areas around the globe. With the help of our innovative and efficient approach to risk assessment, and our risk analysis and monitoring tools, I hope to continue working with financial institutions to effectively mitigate their exposure to money laundering risks.”

—**JENNIFER HANLEY-GIERSCH, CAMS**,
managing partner, Berlin Risk Limited,
Germany



“Professional succession planning, coupled with personal social responsibility, has been always my north. To me, it is key not to rule but to develop and maintain relationships making choices that lead to a more fruitful and socially aware result. The learning and networking opportunities available in our industry are essential to the recognition of new AML/CTF trends that would allow professionals to create meaningful rules or standards for the industry they represent.”

—**KATHALIN CARVALHO, CAMS**, co-chair
ACAMS Central Florida Chapter,
United States



“To play an integral role in raising the accuracy of the detection of money laundering, terrorist financing, and all related financial crimes to support the advancement of future financial crime detection capabilities.”

—**CATHY NANOS, CAMS**,
director of operations,
Financial Crimes Intelligence
Unit, United States

“Working in the private sector of the AML field, what I hope to achieve is not just to ensure compliance with the BSA/AML regulations but also to be able to contribute and establish a true partnership with the government and law enforcement to detect and deter money laundering and other illegal activities. Achieving this would serve the real purpose of BSA and ultimately protect our economy and financial system from abuse by criminals.”

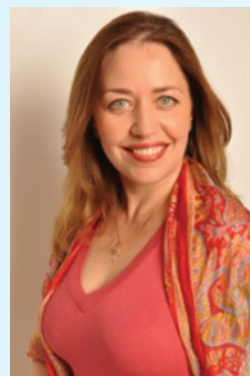
—**MARGARET CHOW**,
CAMS, vice president/
BSA and assistant
compliance officer, The
Bank of East Asia Limited,
United States





“I am really engaged with clients and contacts in order to work towards achieving a better understanding of why AML is important and to connect the dots with the business and day-to-day operations; so that fundamentally, AML is a part of what we do...it is not something else that we do!”

—**JENNIFER FIDDIAN-GREEN, CAMS**,
member of the GTA ACAMS chapter
executive; partner, Grant Thornton LLP,
Canada



“I recently started Radosyn Training and Advisory. Radosyn’s goal is to assist Eastern European countries as well as financial institutions in the Netherlands, in implementing AML and financial crime legislation by sharing best practices through compliance training and advisory. Sustainable businesses require a level playing field, integrity and ethics. At Radosyn we assist in developing and implementing procedures that will contribute to short- and long-term objectives. I believe my work at Radosyn will help contribute and successfully achieve our objectives within the ever-changing landscape of global financial markets.”

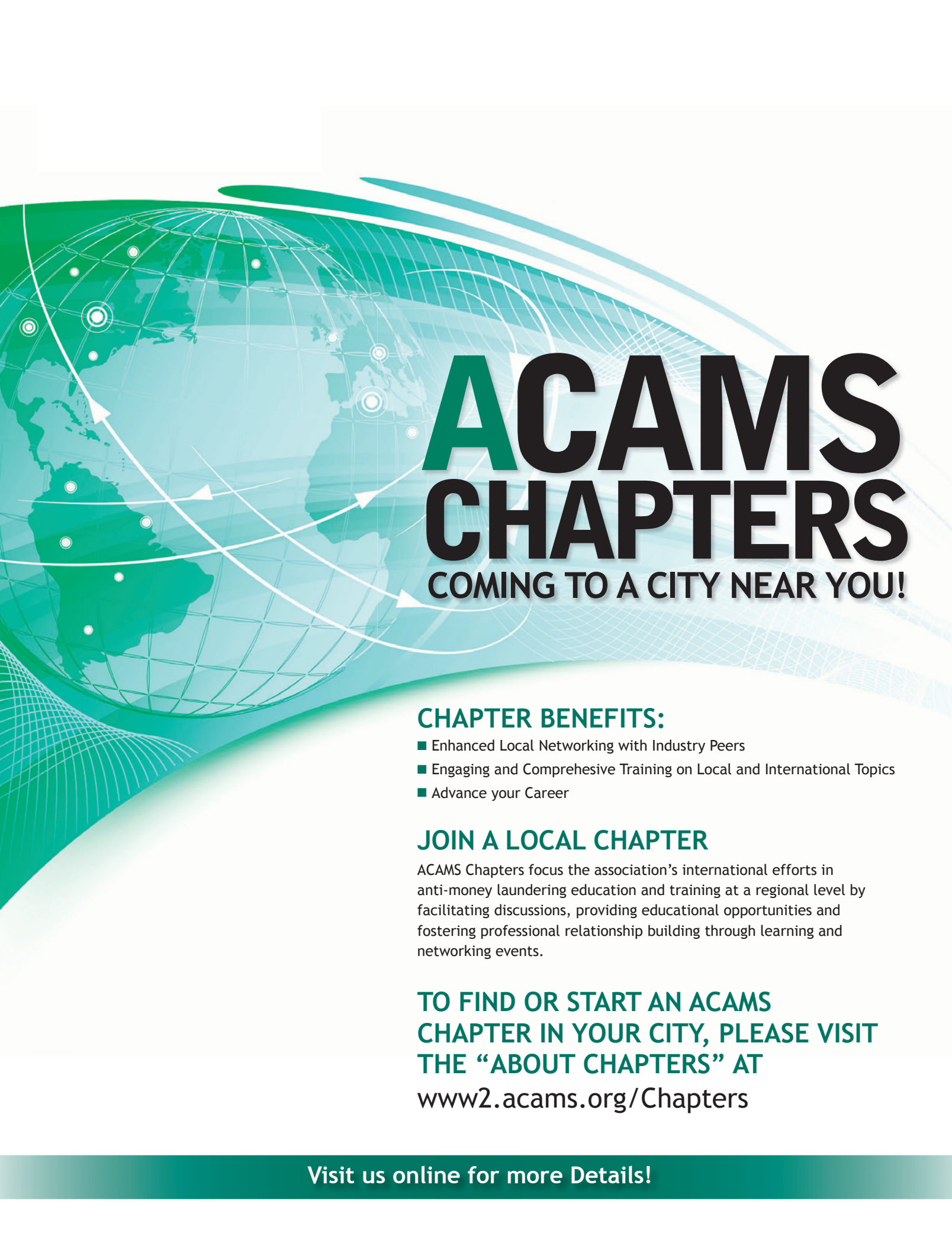
—**YEVGENIYA BALYASNA-HOOGHIEMSTRA, CAMS**,
founding partner, Radosyn, Netherlands

Celebrate
International
Women’s Day 2014
Saturday, March 8



“Our world the one we create through the standards we set and the laws we write will mold the future for our children. I hope to share my knowledge of the malicious ways money laundering affects our society, including heinous acts such as trafficking, and use it to enhance processes, communicate with others, and work together to identify and fight these crimes so the world may be a safer place for all.”

—**ERICA HARPER, CAMS, BSA/**
AML compliance specialist,
MSB Compliance Inc.,
United States



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!

The **why** and **how** of writing a **no-SAR** justification

Suspicious Activity Reports (SARs) are the most valuable external tools that a compliance program provides to law enforcement and regulators in support of the detection and prevention of money laundering and terrorist financing. Identifying, understanding and accurately explaining why a transaction is suspicious are core requirements for every compliance officer. However, does the other side of the coin receive the same amount of attention? As the industry and regulatory environment evolves, it is now critically important to apply the same amount of effort, time and attention to internal justification of why a SAR was not filed. Following is a primer on why “no-SAR” decisions need to be adequately explained and documented and some useful tips on how to develop or improve this process within a compliance program.

Writing the perfect SAR is a frequent subject of articles, white papers, webinars and seminars within the industry. Writing the perfect no-SAR justification is still an emerging art. In fact, so much attention has been focused on SARs, that the no-SAR documentation is often left wanting. The prevailing sentiment within the regulatory world is that this has to change and soon. There are a number of reasons why no-SARs are critical reports.

- Outside inquiries (314, grand jury subpoenas, and law enforcement notices)
 - This is important because filing a SAR is not mandatory simply because the financial institution receives a 314(a) or 314(b) request, a subpoena or other law enforcement inquiry. Retaining investigative documentation to demonstrate that a customer's transactions or activity is not suspicious will provide the rationale for not filing a SAR. Financial intelligence unit (FIU) employees review thousands of customer relationships, and it would be practically impossible for the employee to recall why a

particular customer's activity was not suspicious months or years after investigating that customer's activity.

- Future unforeseen cases — today's “no-SAR” could be tomorrow's SAR
 - The background and investigative work and documentation can provide a framework for the future SAR in the event that the customer's transactions or activity become suspicious at some point in the future.
 - It is important to retain investigative documentation to support the narrative decision to not file a SAR. That documentation will in many cases prove to be important if the customer's activity alerts as potentially suspicious in the future. A change in the customer's activity or transactions does not automatically mean that a SAR is required. However, the historic information that you retain will likely be a valuable asset when you review the customer's activity in the future.
 - If you “don't document it — you didn't do it!”
 - Regulators including The Financial Crimes Enforcement Network (FinCEN) have historically commented that a financial institution's decision to not file a SAR will not be second guessed as long as financial institutions have a well-documented rationale for that decision.

There appear to be different schools of thought as to the level of detail necessary in no-SARs. This is not uncommon within the industry or frankly any reporting system. There are those that believe that every available pertinent detail should be included and those who just want the key decision points and expect the details to be in the supporting documentation. There is no set style and format for creating a no-SAR narrative. While every compliance office may have their own procedures, there are critical elements to



keep in mind. These elements will be very familiar to those who have achieved a high-level of proficiency in writing SARs.

- Think of the audience. What does the auditor, regulator, law enforcement official or any other outsider want and need to see? Craft the justification accordingly.
- Keep it as short and to the point as possible. Make it easy for the reader to find the information they need and move on.
- Make sure that it is clear. Internal jargon and acronyms may mean nothing to those outside of your organization. Be careful about assumptions about the reader's knowledge or experience.
- Make sure that all of the points covered have the appropriate supporting documentation. No decision should appear to have been made on the fly.

Let's explore supporting documentation

- Case files should provide a clear road map of the activity under suspicion at the time it occurred. Remember, make it easy to read and understand. An excellent goal is to never have an auditor or regulator ask, “What does this mean?”

- It should go without saying that documentation needs to be robust and include the same information captured for SAR cases (customer/suspect information, transaction details, evidence of statement review, etc.). This should happen as a matter of course in a normal transaction investigation. Obviously a compliance office needs to collect enough documentation to make the determination that activity is not suspicious; however, in many cases you may have sufficient information without conducting as much investigative work as would be required in a SAR case. For example, the analyst/investigator may be able to determine that the customer's wire transfers are normal for the customer's business and anticipated activity and therefore stop investigating at an earlier stage of the investigation. However, in other cases the investigation may have to continue because the wires may not make sense for that customer, but a later investigative step may reveal that the activity is not suspicious. In other words, the financial institution may not have to exhaust all of the investigative steps in order to determine that the activity is not suspicious.

Some ideas to achieve these goals

- Consider manual procedures/processes and automated procedures/processes in standardizing information capture and retention.
- The compliance officer should have the necessary knowledge and writing skills to meet the content requirements described earlier.
- Clearly define record retention policies and procedures.

No-SAR cases serve as an important source of information captured at the time in which transactions occur. This is why, along with the no-SAR case, financial institutions should seriously consider retaining their associated investigative records. It is common knowledge that financial institutions are required to retain customer transaction records for a period of five years. Yet in many cases the SAR/no-SAR decision is made several months after those transactions occur. For example, a customer conducts transactions on January 2, 2008 and the determination that the customer's activity is made on May 2, 2008. In the event that the financial institution strictly adheres to a five year destruction period, the January 2008 records would

be destroyed at or near January 31, 2013; however, the no-SAR decision was made during May 2008; four months later.

In this case, not retaining the investigative records associated with the no-SAR case could become a problem because critical information associated with the no-SAR case could be lost within the retention period. This highlights the significance of the recording and retention of no-SAR cases because they can become critical information resources in the future at the institution for responding to:


- USA PATRIOT Act (USAPA) Section 314(a) and 314(b) inquiries
- Law enforcement notifications
- Grand jury subpoenas
- National security letters (NSLs)

No-SARs can thus come to bear fruit, as a financial institution (Bank "A") may have had an initial suspicion concerning their customer but may have not been able to obtain enough solid information to meet the criteria for filing a SAR. Meanwhile, another institution (Bank "B") may have had an experience with the same customer whereby a full case was developed resulting in a SAR filing. As well, unbeknownst to either Bank A or Bank B, this same customer could be the subject of a law enforcement (LE) investigation or an ongoing trial, in which case FinCEN data queries based upon the LE investigation generate 314(a) inquiries and ultimately grand jury subpoenas. Furthermore, Bank A could receive a 314(b) inquiry from Bank B or other institutions, should they all be participating institutions in the information sharing program. In each of the aforementioned scenarios, all such inquiries must be responded to by the institution under regulatory requirements.

No-SAR narratives should thus maintain the same high level of quality in detail as those for SAR cases

Those institutions that have implemented strong policies, procedures, and processes pertaining to no-SAR cases, stand the best chance of not only meeting their compliance obligations but serve to make a tremendous and direct impact on the ability of law enforcement to identify, arrest, and prosecute subjects of financial crime investigations. Therefore, no-SAR narratives should thus maintain the same high level of quality in detail as those for SAR cases — the dates, persons, transactions, and details captured in the "no-SAR" narrative may serve as the basis for SAR narratives in the future, should an institution find itself filing a SAR based upon 314/LE/GJ Subpoena/NSL notifications.

Although a financial institution may determine the customer's activity is not suspicious, they may elect to close the customer's relationship because the customer has alerted repeatedly. However, in the event that a customer's account is closed due to the activity in the account, it is highly recommended that the financial institution file a SAR at that point. It is difficult to imagine a scenario where a financial institution would close an account relationship and not file a SAR.

While compliance offices may approach this task differently based on their business environment and regulatory experience, there is no denying that no-SAR justifications are going to come under increasing scrutiny. The compliance office that has this task under control is one that breathes a little more easily when those information requests arrive. 

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

Ed Beemer, CAMS, APR, principal, CorpComm Solutions LLC/ComplianceComm, Arlington, VA, USA, efg@corpcommteam.com

Don Temple, principal, BSA/AML consultants LLC, Fallston, MD, USA, donaldt1@yahoo.com

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

REQUESTING BACKUP



In *The Art of War*, Sun Tzu writes about the importance of knowing your enemy. Unfortunately, we in anti-money laundering (AML) have too often not even taken time to know our friends and allies. Tzu could very well predict the outcome in this situation. One group of allies who are too often estranged from each other in AML are financial institutions' Bank Secrecy Act/anti-money laundering (BSA/AML) investigators, subpoena compliance departments at financial institutions and law enforcement entities engaged in AML investigations.

In traditional law enforcement, record-keeping departments sections are not staffed by personnel with investigative training or prowess. The majority of their often mundane and routine daily functions can normally be accomplished at a lower skill level and expense than that of a trained investigator. If investigators from outside agencies require assistance beyond simple record retrieval, they will likely liaise with an investigator at that agency for that assistance. Subpoena compliance sections at financial institutions functions are very similar. For them, most received requests are often reactive cases and require little more than routine record retrieval. It can be quite different when the investigation is proactive and based on a Suspicious Activity Reporting/Bank Secrecy Act (SAR/BSA) filing. Many of these types of requests include nuances and idiosyncrasies within transactional data that can ultimately make or break a case. Law enforcement investigators need support beyond the abilities of traditional subpoena compliance, but they do not always know where to get this assistance. The logical contact here would be the BSA/AML investigators at the financial institution. Too often, the investigation suffers when law enforcement does not recognize the shortcomings of a subpoena compliance department.

Fostering open lines of communication between BSA/AML sections and subpoena compliance sections can and should be part of investigators' goals, objectives and responsibility. It is a mistake for the BSA/AML investigators at financial institutions to assume that all law enforcement entities are familiar with their existence and responsibilities. Although many will, many other inquiries may come from law enforcement entities and specialties unfamiliar with the extent and scope that BSA/AML now has at financial institutions. Much of the *common knowledge* ACAMS professionals might have, is not that common to law enforcement personnel who have not specialized in this particular area.

Unlike subpoena compliance, AML investigators are responsible for the detection of suspicious activity and the identification of those who engage in questionable banking behavior. This information is documented in a SAR. These SARs identify the 5 W's — who is the client, what type of activity did they engage in, where did the activity occur, when did the activity take place, and (hopefully) why the activity is occurring. The abilities and the know-how of the AML

compliance investigators are the catalysts for minimizing risk on behalf of their respective financial institutions.


Upon documenting the 5 W's, many would argue that the SAR is a complete investigation. Journalists, researchers, even law enforcement would concur that having the answers to those questions constitutes an investigative report. In fact, law enforcement officers take actions such as warrants based on the ability to answer the 5 W's. The question is whether this is the end or just the end of the beginning of an investigation. A law enforcement investigator on the other hand, recognizes that having enough information to obtain a warrant (probable cause) does not mean you have enough evidence for a conviction (beyond reasonable doubt.) The primary mission of an investigator is to conduct a complete and thorough investigation from allegation to verdict. It is the responsibility of an investigator to be accountable for all facets of the investigation.

Law enforcement accountability begins with reviewing SARs to determine if they are viable cases that meet their respective initiative's threshold. When law enforcement investigations are initiated from SARs, the subpoena request normally covers a broad scope of information such as statements, electronic teller journals, cash in/out tickets, date/time of transaction, branch location, signature cards, Know Your Customer (KYC) documents, etc. What is actually received is just a portion of the requested items. Through experience, it takes repeated efforts to secure the originally requested items, thus slowing the investigation as well as the enthusiasm to continue. At times, these critical delays can eliminate the ability to take proactive measures against the target. Although BSA/AML investigators may be aware and sympathetic to law enforcement needs and requests, subpoena compliance departments are often disconnected and less well-trained in investigative and evidentiary needs. What may be obvious to the competent and educated AML investigators has not always been instilled on those in subpoena compliance sections. Bridging this gap and imparting AML familiarity upon the subpoena compliance section begins the necessary mutual aid in order to complete an investigation.

Not having the totality of all the requested supporting documentation to compare to the identified activity, severely hampers the ability of an investigator to articulate the anomaly and make the investigative conclusion obvious to the lay person. A jury is often

made up of lay individuals who now have the awesome responsibility of becoming triers of fact in a court of law. Having a discernible criminal offense is what changes the probability that there was some type of nefarious activity to clear and convincing evidence that leaves the jury panel with the only logical conclusion: Guilty beyond a reasonable doubt. Having all of the requested items help secure the conviction. It is that conviction that not only makes the lasting impact on an offender, but serves as a deterrent to others.

A largely overlooked necessity is identifying not only a point of contact in the SAR, but providing that contact information on the SAR. The ability to directly contact the most appropriate person is advantageous to beginning any investigation. Furthermore, financial institutions often have internal acronyms/names for varying programs/documents that can be beneficial to the investigation. As there is no uniformity amongst the financial institutions, law enforcement may not know to ask for those specific items or if they do know to ask, the name or acronym may not be applicable to all financial institutions. Often when wording is not identical to what that financial institution could provide, that particular requested item is not fulfilled by subpoena compliance. Furthermore, AML compliance investigators clearly have the BSA knowledge as well as the know-how of the internal workings of their respective financial institutions and they are encouraged to edify law enforcement. Conveying internal language will educate law enforcement, and in turn, this knowledge will allow law enforcement to ask for documents in a *language* that can be understood by the subpoena compliance department. Having this universal comprehension allows the subpoena compliance department to immediately recognize what is being asked for by law enforcement and allots for a prompt production of records.

Fulfilling the original offset request in a timely fashion and shipping to the right location, educating law enforcement on the financial institution's internal verbiage, providing guidance to subpoena compliance, can no doubt be tedious but it is this that allows us to reach our mutual goal: Securing a just verdict in a court of law. Retrieval of records is the job description of a clerk, knowing what records to retrieve defines an investigator. 

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

A new approach to adverse media for enhanced due diligence



According to *Psychology Today*, “media studies show that bad news far outweighs good news by as much as seventeen negative news reports for every one good news report.” Several studies also indicate that we care more about the threat of bad things than we

do about the prospect of good things. This is certainly an accurate analogy in the anti-money laundering (AML) world where bad or negative news becomes synonymous with reputational risk.

Identifying customers with high reputational risk is not as straightforward as it may seem. Take for instance the real-life case of a well-regarded Miami attorney who turned out to be a wolf in sheep's clothing as front man for the "Al Capone of Peru." He remained undetected in the customer database of two reputable institutions. This case illustrates the difficulty in exposing hidden risk in the absence of a comprehensive screening program that includes an effective methodology for identifying Reputationally Exposed Persons (REPs). Account relationships with this individual who, on first glance, appeared to be low-risk, could have been prevented. As sanctions and Politically Exposed Persons (PEPs) do, REPs also pose a significant threat to institutions.

Defining adverse media

Adverse media or negative news is unfavorable information that can be found in a variety of reference sources. The risks associated with conducting business with persons or companies having an adverse media profile are many and varied.

While the Federal Financial Institutions Examination Council (FFIEC), the Financial Action Task Force (FATF) and the latest Basel Committee publication of January 2014 do not make specific reference to adverse media in their guidelines and do not provide institutions with standard screening recommendations for Enhanced Due Diligence (EDD), the FATF revised guidelines for AML and Counter-Terrorist Financing (CTF) does mention Internet and media searches for identifying and verifying PEPs. This would suggest that FATF considers negative news monitoring to have some value in identifying potential risk. But herein lies the problem with how financial institutions have interpreted and implemented these guidelines to satisfy the regulators' heightened scrutiny of EDD. The generally accepted approach to finding REPs — those persons or businesses with an adverse media profile — can be limiting.

At the American Bankers Association (ABA) Money Laundering Enforcement Conference last November, a panel on emerging trends in financial crime discussed an approach to compliance using advanced analytics to drive efficiency and effectiveness in an economic climate steeped with challenges. Among the other features mentioned as being relevant for a solid AML program were the need for a "dynamic" client risk rating and a new standard for negative news events with

monitoring ability in real-time. The panel's forward-thinking vision differs to some extent from what is currently in practice by most financial institutions today.

The bucket approach: A traditional view of risk

The traditionally accepted process combines a risk assessment that classifies customers into risk "buckets" of low, medium and high with a "compliant" program to meet basic EDD requirements for ongoing monitoring of high risk. In many cases, institutions will use the Internet and a database of news articles to conduct individual, manual searches for negative news on high-risk customers only. While this type of news product may yield useful information, compliance staff are limited by how many names can be entered manually into a search tool, and by how much time can be dedicated to reviewing potential matches, many of which will refer to people other than the client being investigated. Several shortcomings come to mind when evaluating this traditional methodology:

- Provides only a snapshot of risk, yet customer and web information change daily
- Increases the potential to miss REPs due to the one-dimensional view bucket classifications offer
- Relies solely on human interaction to research and extract information for entity resolution, which is labor-intensive
- Makes it difficult, if not impossible, to stay current with negative news in real-time
- Lacks manageable record keeping and audit capability

Some institutions believe that increasing the number of information sources reviewed will provide additional information that will ultimately lead to more effective risk monitoring. However, the real issue points to human involvement and the passive, static nature of the approach. A broader scope of information does not compensate for a passive system that lacks features for continuous monitoring and notifications when changes occur in customer or web information. Human attention is the increasingly scarce resource relative to computing power and information. Therefore, there is a big difference between a process reliant on user-initiated searches and an automated process that lets an institution know when there is something of interest.

Change comes slowly

An interesting note in a 2013 survey on AML Risk Assessment and Customer Due Diligence indicated that although there has been some conversation within the industry challenging traditional methods for determining AML risk, the majority of respondents conformed to standard criteria (products, services, geography and customer) for performing EDD. Some other noteworthy responses included in the survey were:

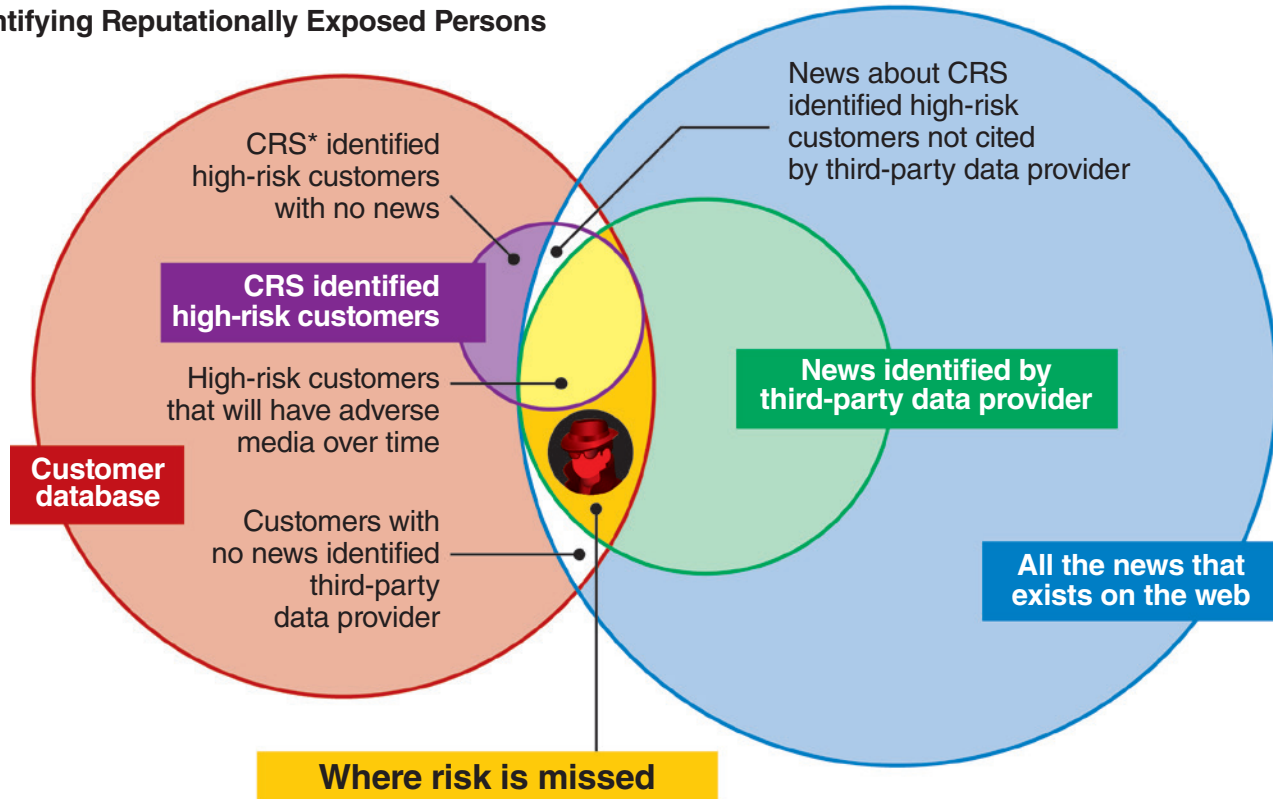
- For most respondents, the need to perform EDD increases as a customer's risk increases; while 5–17 percent of respondents did not view the riskiness of the customer as a trigger to perform EDD.
- When asked to rank types of information and their importance when conducting EDD on a customer, 83 percent of respondents indicated that criminal history was extremely important, 64 percent indicated geography was extremely important and 55 percent of respondents ranked derogatory news as extremely important.
- 67 percent of respondents found news/negative news a helpful source of information when conducting EDD.

Although the survey shows that the majority of financial institutions still conform to traditional methods, it does not necessarily mean that the majority will continue to rule. The regulatory environment in 2014 will be one in which preventing money laundering assumes a broader definition and a greater effort will be made to thwart all types of illegal transactions. More stringent examinations and reporting requirements will not only cover sanctions but also tax evasion and bribery. Meeting minimum requirements will become harder to defend as the focus continues to grow on strong AML, sanctions and anti-bribery processes. The message from regulators to the compliance community has been quite clear as it relates to identifying and closing gaps in their AML programs. In order to do so, institutions must be willing to embrace new ideas and harness the technology that far surpasses minimum requirements.

Shifting the EDD paradigm

A more effective and accurate approach to identifying individuals or entities with adverse media is to use an authoritative, profile-based reference source for identifying sanctions, PEPs and REPs in large-volume databases. The best reference source of this

Identifying Reputationally Exposed Persons



Where risk is missed
Customers not identified as high-risk by CRS process:

- with news cited by third-party data provider
- will have adverse media over time

*CRS — Customer Risk Score

type will usually contain millions of profiles with a rich link structure. This makes it an ideal resource for screening an entire customer database for sanctions, PEPs and REPs and not just customers identified as high-risk by a financial institution's risk scoring process.

Today, the volume of news and the speed at which it changes makes it difficult to keep up. If the bottleneck is the human element associated with news searches, then automation is the remedy. There is a huge difference between investigations that are driven by manual processes and can only be performed on a very limited set of customers, and technology that provides continuous monitoring and notification when information changes.

In the new paradigm, humans are not asking questions but instead are alerted to standing concerns that are being continuously monitored. This becomes possible with technology that marries continuous monitoring

of world news with continuous monitoring of an entire customer database. Benefits of this approach include:

- Can be applied to the institution's complete customer database without jeopardizing EDD guidelines
- Surpasses EDD requirements
- Daily monitoring and surveillance presents a true picture of high-risk and addresses the temporal nature of adverse media
- Establishes a feedback loop to enhance customer risk score processes
- Provides manageable and auditable processes

Conclusion





Complex processes and inconsistencies in the expectations of regulatory agencies will continue to challenge the AML community. With the lack of definitive guidance and standardization, a paradigm shift for EDD is needed now. In the dynamically changing

global environment where individuals and entities operate, one must consider the relevance of their social network or six degrees of separation and the nature and frequency of any related negative media. With the traditional "bucket" assessment, a customer may be categorized as low-risk when, in reality, they have a much higher risk profile once their links and newsworthiness are factored in. By analyzing an individual profile in conjunction with its social network (who they are linked to) and any adverse media direct or through links, institutions can get a more accurate view of risk. Institutions willing to consider non-traditional, innovative approaches to adverse media will have a more effective and efficient process for identifying and managing enterprise-wide risk on an ongoing basis. **A**

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

MEASURING, UNDERSTANDING & EXPLAINING AML RISK

Help your institution:

-  Effectively detect financial crime patterns and spot red flags
-  Mitigate risk and regulatory scrutiny by filling in the gaps in your detection and prevention controls
-  Save time and expense with comprehensive automation and updates
-  Clearly communicate risk through standardized scoring and automated reporting



**For information and to set up a product demo, contact
Tanya Montoya at tmontoya@acams.org.**

AML SYSTEMS: Planning for successful implementation

Those charged with upgrading or replacing a financial institution's anti-money laundering (AML) systems face a complex series of highly inter-related challenges, which will have implications across virtually every aspect of the institution's operations. Proper planning is essential to get it right the first time and avoid delays, rework, budget overruns and the possibility of not meeting regulatory expectations.

In response to increasing regulatory pressures, continuing changes in banking products, processes, practices, ongoing merger and acquisition (M&A) activity, many banks and other financial institutions are re-evaluating the systems used to comply with the Bank Secrecy Act (BSA) and anti-money laundering (AML) regulations. In many instances, this review leads to the conclusion that upgrading or replacing their existing system is the most effective way to both meet regulatory expectations and achieve optimal process efficiencies.

Regardless of the size or geographic scope of the institution, upgrading or replacing these complex systems is a major initiative. Several factors must be considered prior to making the decision, and once the decision is made, careful and accurate planning of activities, resources and time is required for successful implementation.

What drives the need for AML system replacement?

Several industry trends are driving financial institutions to evaluate their existing AML systems and determine if an upgrade or replacement is necessary—including the following:

- **Regulatory scrutiny.** Recent years have seen significantly increased scrutiny from regulators charged with enforcing the BSA and the USA PATRIOT Act. In many instances, regulators are determining

that the systems institutions are using to monitor and mitigate their AML risk are not effective based on the institution's size (including both the number of customers and number of transactions processed), complexity and AML risk profile.

As a result, many banks' legacy systems must be upgraded—and likely replaced with systems that have more sophisticated functionality to help mitigate AML risks and increase the efficiency of the institution's processes.

- **Expansion of products and services.** Existing AML systems are further challenged by the introduction and advancement of new banking products and services. New methods of accessing the financial system can pose major challenges to legacy AML monitoring systems, which must be adapted to include new capabilities for monitoring customer and transaction types that were not in existence when an institution's legacy system was implemented.
- **Increased volume of customers and transactions.** The overall volume of customers and financial transactions has gone up significantly in recent years. Aging AML systems must monitor for more types of suspicious scenarios and examine a larger volume of activity than they were designed to handle.

- **Institutional growth.** As institutions grow—either organically or through M&A activity—they can encounter significant challenges in maintaining compliance with BSA/AML regulations. In the case of organic growth, the institution must determine if its systems are capable of processing and monitoring the increase in customer and transactional data.

In M&A situations, institutions are additionally challenged with the need to process customer and transactional data across several platforms or consolidate data into one platform for consistency and uniformity. For example, a newly unified bank needs to be able to recognize that a customer who had separate accounts at the unmerged institutions is in fact the same customer, even though the customer identification data might vary.

Without proper consolidation of these platforms and their related data, institutions may face gaps in AML monitoring and compliance, as well as increased operational inefficiencies that could drive up operational costs. A consolidation may enable more effective compliance and streamline operations.

- **Aging AML systems.** It is not uncommon for financial institutions to be operating with legacy AML systems that were implemented many years ago. As these AML systems age, organizations might not keep

them up-to-date with the latest software or develop the systems to remain aligned with AML risk profiles. These institutions face a considerably higher risk of being out of compliance due to regulatory changes and changes in their risk profiles. There likely would be the added risk of system failures from which they are unable to recover promptly.

At the same time, software vendors generally decrease the level of support they offer for aging systems as they focus more attention on newer platforms with greater capabilities. Major system upgrades also become less frequent.

Within financial institutions, the trained IT personnel who are most familiar with aging software eventually move on to other assignments or move out of the organization altogether. As knowledge of the system diminishes, the ability to maintain and support it decreases while the associated costs continue to rise.

One additional weakness stemming from aging software relates to the various patches, workarounds and manual “fixes” that accumulate over time. Systems composed of a mix of automated and manual components are not only less efficient to operate but also much more vulnerable to error.

Challenges banks face when upgrading their systems

As financial institutions prepare to implement new and more sophisticated AML systems to meet their specific needs, many find they struggle to determine which systems will meet those needs most effectively. They also are challenged to identify the operational impact of such an implementation and accurately identify the time, effort and resources that will be needed to carry it out. Several areas in particular pose challenges:

- *Understanding regulatory expectations and issued guidance.* The level of scrutiny that regulators give to various types of customer and transactional risks changes over time, as does their focus on particular aspects of AML processes. Institutions must keep abreast of current regulations and regulatory practices.
- *Knowing what capabilities can reasonably be expected from the system.* The capabilities built into AML software programs are updated regularly to keep pace with regulatory changes and new products and services. Banks that are

not completely familiar with the features, functionality and options available run the risk of failing to take full advantage of what the system offers not only from a compliance perspective but to improve operational efficiencies as well.

- *Understanding the complexity and complete project life cycle in order to effectively plan the project.* Replacing or upgrading an AML system is a project of considerable scope and complexity. Most institutions take on such large-scale projects only rarely, making it difficult for them to identify all the dependencies involved, estimate how many resources should be dedicated to it, how long it should take, and what milestones to expect as implementation progresses. Because the various project phases are highly interdependent, the interested groups involved—such as IT, BSA staff, and the various lines of business—must be aligned and coordinated.
- *Allocating available resources while maintaining ongoing operations.* Continuing to operate business as usual during the implementation project is essential to the bank’s ability to maintain compliance and satisfy regulatory obligations. Without proper understanding of the involvement required from its key internal resources, the bank runs the risk of delaying the implementation and opening itself up to additional regulatory scrutiny.

These challenges often take on an extra degree of urgency because of an additional overriding concern: The aggressive timeframe an institution typically commits to for completing the implementation. The schedule might be driven by regulatory bodies or strategic business deadlines.

Planning for the implementation — A comprehensive approach

Choosing the right system and planning properly are important characteristics of successful implementations; in fact, these areas are as critical as the implementation execution itself. A well-defined approach lays the groundwork for minimizing delays, rework and cost overruns.

While approaches and methodologies might vary, some common elements need to be addressed for a successful implementation, including:

- *Vendor selection and contracting.* The fundamental objective is to choose a system that will meet the bank’s regulatory and business requirements. Beyond

this, however, the system selection process must also consider technology requirements such as system security and controls, scalability, flexibility in view of expected growth strategies, expected maintenance requirements, and future upgrade capabilities. It can be helpful to consider the selection process as a series of four phases:

Initiate — Organize the project, finalize the selection strategy and decision criteria and develop a plan for the selection study.

Analyze — Determine specific AML system requirements (both business and technical) and identify possible solution options.

Evaluate — Develop a short list of AML solutions based on stated criteria, vendor due diligence and product demonstrations. Use a consistent scorecard to grade each of the vendor solutions.

Select — Develop a team-endorsed recommendation for presentation to the appropriate decision-makers. Upon approval by the sponsors, begin finalizing contract terms.

- *Implementation planning.* This initial planning is necessary to help the institution better understand the overall costs, timeline and resource needs for such a large implementation. Among the most important planning considerations is the scope of the project— that is, the specific system functionalities to be implemented as well as any customization and additional reporting that must be included to accommodate the environment of the specific institution.

Institutions should also plan how they will accommodate the numerous related needs and the impact that will occur as a result of the implementation. All of the factors listed in the remainder of this section must be considered as part of the planning effort.

- *Data acquisition.* Data acquisition is on the critical path for all AML system implementation projects. Many of the essential activities that must be completed during the course of the implementation are highly dependent on the successful retrieval or integration of data from the bank’s core systems, channel systems, and onboarding systems—which is why sufficient time should be spent planning this aspect of the project.

Acquiring the necessary data might also involve making changes to the bank’s systems. These too must be factored into the budget and resource requirements,

and especially into the project timeline. It is no exaggeration to say that data acquisition can make or break the implementation timeline.

- *Legacy system support during implementation.* Since AML system implementations typically require 12 to 18 months from start to going live, the institution must allocate appropriate resources to keep its legacy AML operation running as effectively as possible during that time. In addition to maintaining existing operations, the institution may also need to accommodate some tactical AML system improvements to temporarily bridge regulatory gaps, demonstrate interim progress to regulators and keep the legacy system running until the new system is live.

- *Resource planning.* A major factor in the timely implementation of the system is planning for adequate internal and external resources.

—*Internal resource needs:* As with any project, the participation of the bank's internal resources is a key consideration because these resources are not typically fully dedicated to the project itself but must function in their daily roles as well. Understanding which of the institution's resources are needed and when and for how long they will be needed enables the institution to use the resources in the most efficient way and to make plans for backfilling the roles needed to complete the bank's daily or business-as-usual activities.

—*External resource needs:* Since implementing a new AML system is not the type of effort that institutions undertake routinely, they often do not have knowledge of or expertise in the system being implemented or the time to spend learning the most efficient way the system can be configured. External resources can be particularly effective in assisting with vendor negotiations, identifying specific components and functionalities that are needed, providing lessons learned and best practices from similar implementation projects at peer institutions, and aiding in understanding the tasks, resources, and effort that will be required to implement the system while reducing risks and avoiding common pitfalls.

—*Post-implementation resource requirements:* With so much focus on the implementation project itself, it is easy to overlook the potential operational impact the new or upgraded system will have after the implementation. In particular, the BSA/AML compliance department will need to consider whether additional staff will be required after the go-live date. For example, in the case of AML monitoring systems, the number of alerts from the new system might increase as a result of implementing additional scenarios. Institutions should begin projecting in advance the adequate number of resources that will be needed to address this increased volume. This will allow them to begin the hiring and onboarding of any additional resources that are required.

- *Testing, validation and tuning.* Before making the transition from the legacy system to the new or upgraded system, the system's functionality, data and integrations will require testing to ensure the results are as desired. In addition, the new system's models and detection scenarios—for example, the transaction monitoring rule scenarios—will require pre-production tuning to be certain the thresholds and parameters for the detection scenarios are set appropriately and can be justified. Planning should account for resources and time spent on both the qualitative and quantitative aspects of creating test plans and test scripts, conducting the tests and conducting the tuning.

- *Model validation.* An AML risk model provides a framework for defining the rules, measurements and scoring that will alert risk managers to situations requiring additional review or investigation. Model validation is the process used to verify that these models are performing as expected. Among other requirements is the written guidance on AML models that the Office of the Comptroller of the Currency (OCC) and the Federal Reserve have issued, which states that “all model components including input, processing, and reporting, should be subject to validation” by an independent third party.¹


As part of the planning of the project, the model governance requirements of the institution must be taken into account.

These include, for example, the guidelines that must be adhered to during model development and any documentation and process requirements that will be required later for model validation. In addition, some institutions may prefer to complete model validation prior to the go-live date. In these instances, the required time must be factored in to determine the overall project timeline.

Awareness and alignment — Critical to success

Replacing or upgrading an AML system is a series of complicated activities that have implications for virtually every operating department of a financial institution. During implementation, banks of all sizes can run into complications, including delays, budget overruns and the costs of regulatory noncompliance.

Anticipating and avoiding such pitfalls requires a broad range of planning, preparatory, management, and communication activities and coping with the many complexities beyond the selection of an AML system vendor. It is particularly important that all those involved—including the BSA/AML compliance team, the IT department, and the individual lines of business—be fully aware of the critical nature of the implementation project and the significant consequences that can follow if the project falls short of compliance or process requirements.

Finally, an initiative of this magnitude and complexity requires strong leadership by executive-level sponsors. It must demonstrate its own commitment and participate actively, by establishing and communicating the overall vision, providing the required resources, and seeing that important issues are addressed and resolved. 

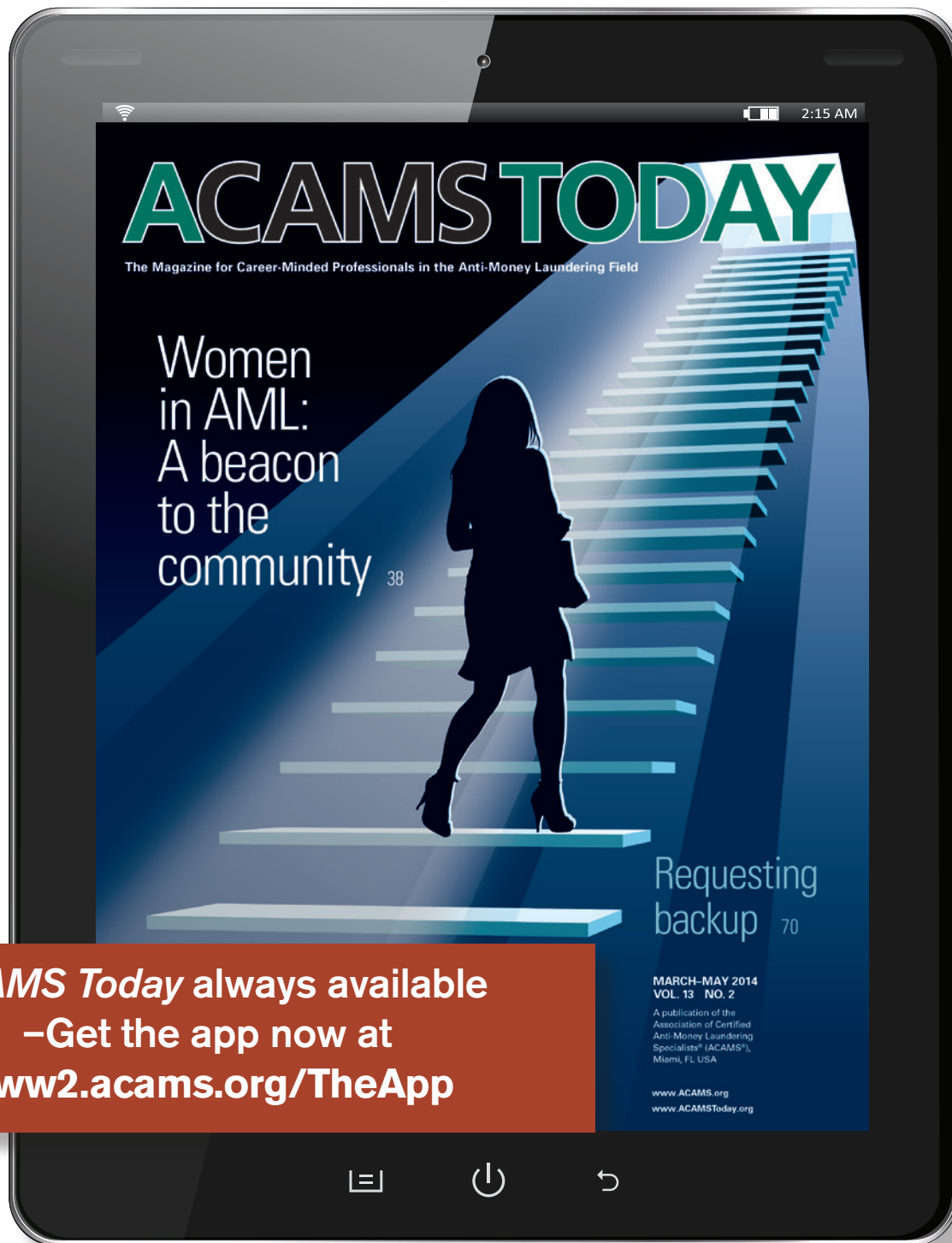
Brookton Behm, principal, Crowe Horwath LLP, Grand Rapids, MI, USA, brookton.behm@crowehorwath.com

Nick Grove, Crowe Horwath LLP, Washington, D.C., USA, nick.grove@crowehorwath.com

Tapán Shahis, Crowe Horwath LLP, Chicago, IL, USA, tapan.shah@crowehorwath.com

¹ See Brookton N. Behm, John A. Epperson, and Arjun Kalra, “AML Model Risk Management: Meeting Examiners’ Rising Expectations,” Crowe Horwath LLP, June 2013, <http://www.crowehorwath.com/ContentDetails.aspx?id=6350>

Now **AT** Your Fingertips!



**ACAMS Today always available
–Get the app now at
www2.acams.org/TheApp**



ACAMS Today, the elite magazine dedicated to enhancing the skills and knowledge base for the financial crime prevention professional.

www.ACAMSToday.org

Goldilocks and the three sanctions



In the fairytale, the little girl named Goldilocks had a choice of three beds in which to take a nap. The father's bed was too hard, the mother's was too soft, and only the baby bear's bed was comfortable enough for her in which to fall asleep. In a similar fashion, economic sanctions programs can either be ineffective, achieve their desired goals, or be so punitive as to possibly backfire.

Economic sanctions are enacted to achieve one of a number of goals, some unacknowledged in public:

- To express disapproval of specific conduct (including to citizens of the country imposing sanctions)
- To make it more difficult for sanctioned entities to continue the unwanted conduct
- To provide economic incentives for sanctioned entities to change their conduct

To be effective in effecting changes in behavior, the parties imposing sanctions have to exert leverage over the sanctioned parties; otherwise, there is neither a penalty nor an incentive for change.

Too soft: Guinea-Bissau and Cuba

The tiny West African country of Guinea-Bissau may be unknown to many *ACAMS Today* readers. It has had a tumultuous history since gaining independence from Portugal in 1974. There have been no less than five coups or presidential assassinations

in the 40 years that the country has existed. The most recent coup, in 2012, resulted in United Nations sanctions, which were then also enacted by the European Union, Economic Community of West African States (ECOWAS), the U.K., Canada, Australia and Switzerland. Notably absent from that list is the U.S. Why?

The Office of Foreign Assets Control (OFAC) has not sanctioned Guinea-Bissau, in part, because it has no leverage to effect change. According to government web sites, the small country is the U.S.' 195th largest trading partner — in other words, one of the smallest. In 2010, for example, 0.95 percent of Guinea-Bissau exports crossed the Atlantic to the U.S. Enacting sanctions, while expressing disapproval, would not provide the incentive for the government to mend its ways.

So, are the sanctions likely to be effective, even in the absence of the U.S. involvement? In a word — no. This is partially because the one country that might have leverage over Guinea-Bissau has not enacted sanctions against it. In recent years, India has regularly been the destination of the majority of Guinea-Bissau's exports. The tiny country primarily exports nuts and fish and has become the world's sixth largest producer of cashews, a staple of Indian cuisine.

Even if India were to prohibit trade with Guinea-Bissau, there is no guarantee that this would cause the military leaders to change course. The country is one of the

poorest in the world; it is unclear that further damage to its economy would have much meaning to a populace that has so little to begin with. So, perhaps not even India has leverage over the ruling junta.

The Caribbean nation of Cuba presents another vivid example of sanctions that do not achieve their aims. The U.S. has maintained some level of sanctions since it embargoed trade with Cuba in the wake of the Cuban Revolution deposing the Batista government, and the nationalization of the substantial business assets owned by American concerns in its wake. The Cuban government was sanctioned under the Trading with the Enemy Act, and the Cuban Assets Control Regulations issued by OFAC, in 1963. And, while Cuban sanctions laws, such as the Cuban Democracy Act of 1992 and the Cuban Liberty and Democratic Solidarity Act of 1996, implore other nations to apply the same standards to the Castro regime as it has done to other governments who commit human rights abuses and suppress democratic opposition, for over 50 years, the U.S. is alone in sanctioning Cuba.

It is undeniable that the sanctions have had economic repercussions for both countries. The Cuban government estimates that the embargo costs the island nation \$685 million annually, while the U.S. Chamber of Commerce estimates that the U.S. economy is denied \$1.2 billion each year.

However, as trade between Cuba and other countries continues unabated (even the U.S. is responsible for over 6 percent of Cuban imports, albeit on cash terms only), while the sanctions impose hardship on the Cuban people, it has proven insufficient to encourage changes of behavior, especially over such a long period of time.

So, why are there Cuban sanctions, if they have proven ineffective in changing behavior, and have no realistic prospect for doing so? The simplest explanation is the most likely: The sanctions exist because they serve a political purpose in the U.S. There is political value in sanctioning a Communist regime just off the Florida coast, especially one that expropriated sizable amounts of American assets, and once briefly housed Russian nuclear missiles — especially with the sizable Cuban expatriate community in South Florida.

Just right: Burma

On the other hand, a truly illustrative example of how sanctions can be effective lies in the Myanmar (formally known as Burma) sanctions program. As a consequence of suppression of opposition to the military junta, which rules the country, sanctions were imposed and strengthened through much of the 1990s and 2000s by both the E.U. and the U.S. Most notably, after violent suppression of anti-government protests in 2007, the E.U. and U.S. banned imports of jadeite and rubies mined in Burma, one of the country's main exports.

The military rulers reacted to the impact on the economy by, over the next few years, effecting changes to make Myanmar a more pluralistic society. Most notably, in November 2010, they released Aung San Suu Kyi, the prominent opposition leader who had been subjected to extended periods of house arrest totaling 15 years.

Although there was no notable sanctions relief immediately after that event, the U.S. initiated secret negotiations with the junta and ignored recommendations of the U.S. Embassy in Yangon to add hundreds of additional names to OFAC's Specially Designated Nationals (SDN) List for 3-1/2 years.¹

Continued progress toward democracy did result in the suspension of E.U. sanctions and significant reduction in U.S. sanctions in 2013.

Even in the face of this detente, however, OFAC has recently designated an individual and three entities for their involvement in arms trade with North Korea. This second category of sanctions against Myanmar was originated through the issuance of Executive Order 13619 in 2012, and serves as a warning that being accepted as a "good actor" includes both the internal and external conduct of a government.

Too hard? Decades of Iranian sanctions

The history of sanctions against Iran has run the gamut from originally being "too soft" to potentially becoming "too hard." While the U.S. originally sanctioned Iran after the storming of its embassy during the Carter administration, the current set of sanctions were first promulgated in 1987. The focus of those restrictions was based on Teheran's support of terror groups, most notably Hezbollah.

Although the U.S. tightened the sanctions again multiple times in the late 1990s, it acted alone against Iran, with no visible effect until 2007, when Teheran's apparent nuclear ambitions started to draw sanctions from the U.N. and E.U., among others.

Still, despite the greater unanimity, the sanctions resulted in no apparent response from the Iranian government because Iran retained its primary source of revenue, and leverage — oil. Once sanctions regimes included restrictions on the Iranian energy sector in 2012, the economic pain in Iran grew great enough that the next presidential elections went to Hassan Rouhani, a moderate. Perhaps more notably, the Islamic clerics who truly control the government gave the new leader some leeway to negotiate sanctions relief in return for reforms to the sanctions imposed on Teheran.

Even so, as the six-month confidence-building arrangement between Iran and the P5+1 (U.S., U.K., China, Russia, France, and Germany), known as the Joint Plan of Action, takes effect, there are storm clouds forming in the U.S. Congress that have the potential for sanctions on Iran to go beyond effective to being counterproductive. Legislators from both parties believe that the current interim deal does not go far enough in rolling back the threat of Iranian nuclear weapons capability, and that the threat of even harsher sanctions will produce an even better negotiated result. Are they right,

or could adding insult to injury scuttle the whole deal — or worse?

When is enough enough?

Can sanctions be too punitive, and produce the opposite of the desired result, perhaps years or decades later? The Treaty of Versailles, which ended World War I, offers a compelling argument that pushing Teheran beyond what has already been agreed to could come back to haunt the U.S. The Treaty imposed harsh financial penalties, as well as significant territorial concessions, on Germany. It was imposed, rather than negotiated. The German people considered it a "Diktat" (a dictated solution) rather than a negotiated end to the war, and came to see the Weimar government who agreed to it as traitors. The German economy suffered, particularly after the French invaded the Ruhr valley when reparations payments went into arrears. In such an environment, the humiliated populace turned to those who could return a sense of national pride and improve their lot. That, of course, was the National Socialist Party — the Nazis. Common wisdom, according to numerous available analyses of the post-World War I period, draws a straight line from the harsh terms of the Treaty of Versailles to World War II — in the span of only 20 years.

You made your bed...

Sanctions programs, to be effective, need to have leverage to achieve their aims. If the restrictions do not make a major impact on how those who are sanctioned conduct their daily business, and does not change their assessment of their longer-term future, there is no incentive to change course.

On the other hand, pushing one's advantage beyond that which is necessary may result in unintended consequences down the road. When persuasion turns to coercion and beyond, sanctioning countries can become demonized.

Perhaps, those who impose sanctions should recall that Goldilocks only slept soundly when she found the bed that was neither too soft nor too hard. **A**

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

¹ Erika Kinetz and Matthew Pennington, "AP Impact: Burma List Languishes", AP News, 18 May 2013, 20 January 2014 <<http://bigstory.ap.org/article/ap-impact-myanmar-sanctions-list-languishes-0>>

SINGAPORE



– PICKS UP THE PACE IN COMBATING ECONOMIC CRIME

Like the other three Asian Tigers — Hong Kong, Taiwan, South Korea — Singapore has developed into one of the most advanced and high-income economies in Asia. Singapore has become one of the world-leading international financial centers. Although reports state that Singapore reportedly benefits from the regulatory attack on established financial centers, like London, New York and Zurich, it also appears that Singapore largely benefits from growth within the Asian region as a whole. Some media reports claim that the city-state of Singapore is likely to become the world's second-most important offshore center, after Switzerland, by 2017.

Singapore's exposure and its reaction to acts of economic crime

According to the 2013 U.S. State Department Money Laundering Report, Singapore is a major international financial and investment center as well as a major offshore financial center. The report stated that secrecy protections, a lack of routine large currency reporting requirements, and the size and growth of Singapore's private banking and asset management sectors pose significant risks and make the jurisdiction a potentially attractive money laundering and terrorist financing destination for drug traffickers, transnational criminals, foreign corrupt officials, terrorist organizations and their supporters. As reported by the *Spiegel Online*, in November 2013 Singapore strives to retain its attractive financial center while preserving its reputation as a corruption-free zone and remaining a level above pure tax shelters. It has therefore been keen to meet international regulatory standards in the area of anti-money laundering (AML) and other economic crimes like tax evasion.¹

¹ <http://www.spiegel.de/international/world/the-singapore-banking-sector-is-a-tax-haven-that-now-faces-reform-a-930998.html>

Singapore has been involved in a number of scandals surrounding allegations of cross border tax evasion and money laundering, involving individuals, corporations and politically exposed persons (PEPs). The cases published by non-governmental organizations (NGOs), media sources and investigative journalists are summarized below. Between 2010 and 2013 the Singapore Monetary Authority (SMA) made 108 inspections related to AML and terror financing controls on financial firms. According to an article published in the *South China Morning Post*, Singapore's central bank fined 22 financial institutions and restricted operations at seven for failing to comply with rules to prevent money laundering and terrorism financing for the same period.²

- **India** — In May 2012, the Indian ministry of finance described Singapore as a “tax haven” in its white paper on Black Money. The report accused Singapore as acting as conduits for foreign direct investment (FDI) into India and alleged that Singapore was assisting individuals and corporations in avoiding taxes and concealing the identities from the revenue authorities of the ultimate investors, many of whom could actually be Indian residents, who have invested in their own companies, through a process known as round tripping. As reported in the *Singapore Independent*, Singapore's Prime Minister Lee Hsien Loong, stated that Singapore did not have any interest in being a money laundering center and added that he did not think that any shady money would want to come to the city-state. He was quoted as stating: “I think shady money would rather go somewhere else rather than risk being scrutinized by our regulators.”³
- **Myanmar** — Allegations that Myanmar's former military junta has stashed billions of dollars in Singapore surfaced again in October 2013. Like with former allegations, they were dismissed each time both by the Myanmar and Singapore governments. The financial institutions mentioned in these unconfirmed rumors were the Overseas Chinese Banking Corporation and DBS Group.

- **China** — In January 2014, *The Independent* reported that relatives of senior Chinese officials including President Xi Jinping and former premier Wen Jiabao are allegedly using offshore tax havens to hide their wealth. Two offshore companies identified as a result of the investigation undertaken by *The International Consortium of Investigative Journalists* identified, one based in Singapore, Portcullis TrustNest, and Commonwealth Trust Limited in the British Virgin Islands (BVI) allegedly helped well-connected Chinese clients set up offshore companies, trusts and bank accounts.⁴

- **Thailand** — *The International Consortium of Investigative Journalists* has published a number of reports on tax havens and offshore centers. According to a report titled: “Secret Files Expose Offshore's Global Impact,” a Thai government official with links to an unnamed African dictator used Singapore-based TrustNet to set up a secret company for herself in the BVI.⁵

- **Malaysia** — In March 2013, London-based campaign group Global Witness presented a “sting” video in which a person posing as a foreign businessman is seen negotiating with purported relatives and associates of state chief Taib Mahmud who has headed the resource-rich Sarawak on Borneo island as chief minister since 1981. In one part of the clip a man introduced as a Taib family lawyer called Singapore “the new Switzerland” with a “China Wall” protecting the identities of Malaysian depositors. Mahmud has reportedly over a period of many years denied allegations of large-scale corruption and nepotism. The 16-minute video alleged that Mahmud's relatives and associates get massive tracts of land at bargain prices from the state, sell companies owning the land titles to foreigners, and then take payment in Singapore to evade taxes.

Singapore's efforts to combat tax evasion

In 2009, Singapore endorsed the OECD tax standard on the automatic exchange of information and integrated it into all double taxation treaties. Since July 1, 2013, tax evasion

and tax fraud have been designated predicate offenses for money laundering. Singapore is due to conclude an inter-governmental agreement that will facilitate Singapore financial institutions' compliance with the American Federal Account Tax Compliance Act (FATCA) law. But the new, stricter laws only apply to taxes the city-state collects. Singapore has neither inheritance nor capital gains taxes.

Singapore has neither inheritance nor capital gains taxes

Singapore-based financial institutions are currently required to conduct customer due diligence to deter and detect proceeds from serious foreign tax offenses, even if they are not offenses in Singapore. In May 2013, Singapore signed the OECD Multilateral Convention on Mutual Administrative Assistance in Tax Matters, in order to enhance the international cooperation on the exchange of tax related information.

The government has also proposed to amend the Income Tax Act so as to allow the Inland Revenue Authority of Singapore (IRAS) to obtain bank and trust information from financial institutions without having to seek a court order. Also in 2013, Singapore and the U.S. concluded an inter-governmental agreement that will facilitate financial institutions in Singapore to comply with FATCA, a U.S. law which requires all financial institutions outside of the U.S. to pass information about financial accounts held by U.S. persons to the U.S. Inland Revenue Service on a regular basis.

² <http://www.scmp.com/business/companies/article/1281461/singapore-fines-22-firms-money-laundering-over-past-three-years>

³ <http://theindependent.sg/singapore-tax-haven-or-not/>

⁴ <http://www.icij.org/offshore/china-who-uses-offshore-tax-havens>

⁵ <http://www.icij.org/offshore/secret-files-expose-offshores-global-impact>

Singapore's efforts to combat money laundering and tax evasion

In January 2014, Singapore issued its inaugural national risk assessment (NRA) report on money laundering and terrorist financing risks in the country.⁶ The assessment covered 14 financial sectors such as full banks and money changers, and eight non-financial sectors such as casinos and money lenders. The report, which presented the results of the NRA noted that many sectors have in place a robust regime to combat money laundering and terrorist financing and underlined that Singapore's AML and counter-terrorist financing (CTF) regime is grounded in tough regulations, rigorous supervision and effective enforcement. The report also highlighted several sectors potentially vulnerable to money laundering and terrorist financing. According to the assessment, internationally-oriented and cash-intensive sectors are particularly exposed to the risks, the report found. Although full banks face higher inherent risks, owing to their large customer volumes and the international nature of their transactions, the report underlined that controls in banks are the most developed. Singapore is Asia's largest private

banking center with offshore assets of reportedly about \$800 billion leaving this area of banking also exposed to increased risks. The report also noted that there is room for improvement in the areas of trade finance and correspondent banking. Also, according to the study accountants and other corporate service providers can be exposed to money laundering and terrorist financing activities if higher-risk customers hire them to set up complex structures that conceal ownership and reduce the transparency of transactions.

In the non-financial sectors, corporate service providers like law and accounting firms are also a sector with a higher level of money laundering and terrorist financing risks. In response, the Accounting and Corporate Regulatory Authority has proposed new legislation that will come into effect in 2014. In the same year, the Insolvency and Public Trustee's Office aims to introduce a new regime for the sector in 2014 to strengthen the fast growing pawnbrokers sector. According to the report, emerging issue areas for further study included virtual currencies, which currently lack a set of global regulatory standards, and the Singapore Freeport, a storage vault for valuables launched in 2010.

Conclusion

Although Singapore has been criticized as being the new tax haven, recent regulatory measures and legislation coming into force has shown that Singapore is intent on maintaining its standing as a reputable and stable financial services center. The government has set the tone for high standards and it does not appear to be slowing down the momentum of fulfilling international best practice standards in combating economic crime. Singapore's score on international rankings for corruption, currently number five on the list of least corrupt countries in the world, clearly provides a solid basis on which to build an effective AML regime.⁷ Nonetheless, given Singapore's offshore status, undertaking risk-based customer due diligence — in particular for foreign PEPs and intransparent corporate vehicles, time is of the essence for financial institutions and corporations in order to mitigate the risks of money laundering effectively. **A**

Jennifer Hanley-Giersch, CAMS, managing partner, Berlin Risk Limited, Berlin, Germany, jennifer.hanley@berlinrisk.com

⁶ The full report can be viewed under the following link — http://www.mha.gov.sg/news_details.aspx?nid=MzA3Nw==&dlky22HZAc=

⁷ <http://cpi.transparency.org/cpi2013/results/>

YOUR AD HERE

Don't miss your opportunity to reach a readership of over 20,000 AML professionals

TO ADVERTISE HERE

CONTACT ANDREA WINTER:

1.786.871.3030

AWINTER@ACAMS.ORG

ACAMS® Advancing Financial
Crime Professionals
Worldwide

INTERVIEW WITH CHIEF COMMISSIONER OF MACC



A *CAMS Today* had the opportunity to speak with Tan Sri Abu Kassim Mohamed, chief commissioner of the Malaysian Anti-Corruption Commission (MACC). Tan Sri Abu Kassim was appointed by His Majesty the Seri Paduka Baginda Yang di-Pertuan Agong upon the advice of the Prime Minister in accordance to Section 5 (1) of the MACC Act 2009. The chief commissioner is assisted by three deputy chief commissioners — operations, management & professionalism, and prevention in performing the prescribed duties and responsibilities.

Kassim joined the civil service in September 1984 upon completing his degree in Social Sciences from Universiti Sains Malaysia (USM), Penang. Upon entry into the civil service, he was posted to the then Anti-Corruption Agency or ACA, as it was commonly known, as an investigation officer. In 1989, he furthered his studies by pursuing a bachelor's degree in Criminal Justice at the Michigan State University in the U.S.

He made his way up from an investigation officer in 1984 to the director of the planning and policy coordination division in 1999. He then moved on to become the director of anti-corruption agency for the state of Perak in the year 2000 and the state of Penang in the year 2003. In 2005 he was appointed as director of the newly establish Malaysian Anti-Corruption Academy (MACA). He was the director of MACA until May 2006 before being appointed as chief integrity officer at Amanah Raya Berhad. In 2007 he was appointed deputy director general I of ACA. In 2009, he took responsibility as deputy chief commissioner of the MACC. Kassim was appointed to his current position as chief commissioner of MACC on the 1st of January 2010.

Besides his remarkable career progression, he participated in numerous anti-corruption activities and networks. He is member of the INTERPOL Group of Experts on Corruption (IGEC) since 1997. He is furthermore involved in the process of preparing the code of ethics for law enforcement, a best practices guide for INTERPOL members and the Global Standard to Combat Corruption in Police Services. Kassim presented numerous working papers relating to the fight against corruption, inter alia "The Fight Against Corruption: A Collaborative Approach Between MACC and MACA in Combating Corruption," which was introduced at the 78th General Assembly Session in Singapore in 2009.

Internationally, in the year 2006, Kassim was appointed as a member of the executive committee of the International Association of Anti-Corruption Authorities (IAACA) and in the year 2013 he was appointed as vice president of IAACA. In 2012, Kassim was also elected as a member of the board of governors of International Anti-Corruption Academy (IACA) in Vienna for a six years term. Prior to that, he was member of International Academic Advisory Board of IACA.

Moreover, Kassim is also engaged in the academic field. He is currently an adjunct professor of education and social science

faculty at the University Industry Selangor (UNISEL) and University Teknologi MARA (UiTM) in Accounting Faculty. Kassim is also on the board of directors of the Institute Integrity of Malaysia and a member of advisory panel for Malaysia Company Commission Training Academy.

ACAMS Today: What is the mission of MACC and its interactions with government departments relating to the AML issue?

Tan Sri Abu Kassim: The MACC plays important roles to ensure that we can combat the anti-money laundering (AML) issue more effectively and comprehensively. For this reason, the MACC is working closely with other government agencies such as AG Chambers, Bank Negara Malaysia (BNM), Inland Revenue Board, the police and customs. We need to have a good, strong cooperation with all respective departments; otherwise, we can't win this war.

In this regard, attention should be placed on the existing law in dealing with financial crimes like money laundering. In Malaysia, the AML and Anti-Terrorism Financing Act 2001 has been enforced since January 15, 2002 to curb any money laundering activities through provision of money laundering offenses, measures to prevent money laundering and terrorism financing offenses, as well as asset forfeiture. After more than a decade of enforcement, AML and Anti-Terrorism Financing (Amendment) Bill 2013 was brought to Parliament for the first reading last December. It was informed that the bill would be debated in the coming Parliament session in March. The amendment will give additional power to strengthen the financial system in Malaysia. We learned that the integral component of the revised AML policies is the introduction of an obligation for reporting institutions to adopt a risk-based approach in identifying, assessing, and understanding money laundering and terrorism financing risks of respective reporting institutions. I think this is a good move.

As a sole anti-corruption agency in Malaysia, the MACC always maintains valuable interactions with government departments to manage AML issues effectively. We have formed the National Coordination Committee to Counter Money Laundering (NCC) and also Special Task Force. Both entities meet frequently to discuss all the necessary action actively. Active interactions and concerted effort are vital. The NCC — comprised of members from 16 government agencies — oversees and coordinates government-wide AML efforts.

Since 2000, Malaysia has made significant progress in constructing a comprehensive AML regime. This significant progress comes from the strong cooperation between the agencies. We hope this cooperation will be strengthened further in the coming years and the MACC hopes to play a vital role in the prevention of corruption and money laundering activities.

I would also like to share remarks from the UNDOC' Review Report, which was released last year, to show the close and strong rela-

Significant progress
comes from the
strong cooperation
between the agencies

tionship between government agencies. The report stated that the MACC has memoranda of understanding (MOUs) in place with several institutions and receives reports, from among others, the Public Complaints Bureau, the FIU of BNM, and the Auditor General, and also Royal Malaysian Police (RMP), who was also responsible for the investigation of money laundering, including predicate offenses regulated in the AML and Anti-Terrorism Financing Act (AMLATFA). This report also said that the MACC with other Malaysian law enforcement agencies such as the RMP, AG Chambers and FIU exhibit a high level of commitment to the fight against corruption and cooperation internationally, and to fully implementing the principles of the convention, in particular at the leadership levels of the agencies.

AT: What is your vision for MACC's development and its role in anti-corruption, money-laundering prevention and financial crime investigations?

TSK: As all of us know, the war against corruption is getting more complex compared to the 1990s. We can also see similar scenarios in preventing money laundering and financial crime investigations. We need to face these challenges. And, it

is not an easy task. Thus, our vision is very clear. In strengthening cooperation with other agencies, I want to see the MACC be the main center in combating and tackling these issues, especially in the anti-corruption and money-laundering sectors. Of course the financial crime investigations are part of this process. As I mentioned earlier, corruption, money laundering and financial crime 'work hand-in-hand' and we need to tackle this problem completely. To achieve this objective, we need to strengthen our investigative infrastructure, including having a better legal system, having competent, skilled and trained staff and developing a better training module according to current needs.

AT: What are some of the critical anti-corruption and AML challenges facing Malaysia and Asia? What advice would you give on how to best deal with these challenges?

TSAK: Malaysia and Asia are not the only ones facing the challenges, but other regions and other parts of the world are as well. Here in Malaysia, we are facing at least three challenges, namely international liaison, cross-border crime and mutual legal assistance. We need to give high level consideration to overcome these challenges; otherwise, we can't win the battle against corruption, money laundering prevention and financial crime in a holistic manner and both at a domestic and international level. We need to have better and effective ways, which can only be achieved through a strong cooperation between nations.

For example, we must have a better mutual agreement on sharing financial information. We in Malaysia, I should say, are facing problems obtaining information about financial transactions, although we have MOU in combating corruption with eight countries and anti-corruption agencies. We need to have and should have better cooperation if we really want to combat corruption, money laundering prevention and financial crime effectively. If not, we will only end up talking, formulating plans and strategizing action, but fail to win the war at the end. Apart from that, we also need to have a better cooperation to solve the issue of dual criminality. Under this provision, we hope that any offenses convicted in Malaysia should also be considered as offenses in the country of the convict.

As we know, according to the dual-criminality principle, a person may be extradited only when his or her actions constitute an offense in both the requesting and requested states. Under the rule of dual-criminality,

an extraditable offense must be punishable under the criminal laws of both the surrendering and the requesting state.

Here, I would like to share some points highlighted by International Transparency UK in its report under the title "Combating Money Laundering and Recovering Looted Gains." According to the report, "Over the years Commonwealth heads of Government have adopted a number of documents that enshrine good governance and help the fight against corruption. All the same, Commonwealth states have continued to be blighted both by the siphoning or looting of state assets by ministers or senior officials, and the widely varying legislative and procedural effectiveness of their anti-corruption measures. The Commonwealth Heads of Government meeting in Vancouver in 1987 endorsed the Harare Scheme for Mutual Assistance in Criminal Matters within the Commonwealth which had been agreed the previous year. The purpose of the Scheme was to increase the level and scope of assistance rendered between Governments regarding a fairly comprehensive range of actions, many of which would now be covered in the UNCAC. However, the Scheme is a voluntary arrangement, and not a formal instrument, and there is the expectation that a Commonwealth state will render assistance to another based simply on its provisions."

As said by that report, one of the main hindrances faced by asset recover and money laundering investigations is the inability of some states to make or execute mutual legal assistance (MLA) requests in a timely and effective way. This implies that a level of specialization in international cooperation matters needs to be developed within small states, as well as the establishment of international networks between prosecutors and investigators that will enable requests, both formal and informal, to proceed without delay.

Moving from this, we feel that we should adopt a wider effective arrangement, especially in terms of dual-criminality and cross-border crime between countries to fight corruption, money laundering and financial crime. Malaysia, as a member of the Anti-Corruption Initiative for Asia and the Pacific/Organization of Economic Co-operation and Development (ADB/OECD), the South East Asia Parties Against Corruption (SEA-PAC) mechanism, the Asia Pacific Economic Cooperation (APEC), Anti-Corruption and Transparency Working Group, the Asia Pacific Group (APG) on Money

Laundering, the Offshore Group of Banking Supervisors, the Egmont Group of Financial Intelligence Units, the International Association of Anti-Corruption Authorities (IAACA), the International Anti-Corruption Academy (IACA), INTERPOL, and ASEANAPOL, I hope this would be materialized. We also hope that member parties of UNCAC, Financial Action Task Force (FATF), Asia/Pacific Group on Money Laundering and Egmont Group of Financial Intelligence Units (FIUs) could work more closely toward having a better and effective platform.

AT: In the last five years, what would you say are the most memorable anti-corruption lessons and how have these lessons impacted the AML space and the compliance professionals working in those areas?

Anti-corruption and
anti-money laundering
are becoming very
complex nowadays

TSAK: Since the formation of MACC in 2009, we have witnessed many changes and have experienced a series of lessons. The changes and improvement are a result of the MACC Transformation Program. Among others are the formation of Anti-Money Laundering Branch in Investigation Division and also the establishment of Special Operation Division and Forensic Accounting Division. Both divisions are important to have a better investigation process, which includes AML investigations. As mentioned earlier, anti-corruption and AML are becoming very complex nowadays. So, we need competent, skilled and professional investigators. We need to prepare for this. Thus, under the transformation program, we are taking all necessary measures to achieve these objectives. This includes taking people from the private sector, and they, apart from helping us in terms of conducting forensic investigation, will also assist MACC to develop a stronger staff.

AT: What counsel would you give to financial institutions on how to build a solid anti-corruption and AML compliance program?

TSAK: One of the new initiatives that the MACC carried out via the transformation program is the private sector investigation. Corruption and money laundering involves members from public and private sectors. This is the reality. We need to take all the necessary steps to include compliance programs in all sectors. As I mentioned earlier, we want the MACC to play a role as a main center in combating money laundering activities in Malaysia.

Back to your question, what is my advice or counsel to the financial institutions, my advice is simple. The financial institutions should have a complete AML compliance program, robust internal audit mechanism, and continuous review of risk and compliance policy. They should consider having an internal integrity unit. Latest survey findings including KPMG's Fraud, Bribery and Corruption show that we are at the right junction to have a better, stronger and more effective compliance program. We hope to incorporate a new provision— a corporate liability clause will be included in the MACC Act by this year. We strongly believe that the new provision needs to be supported by proper internal control systems or mechanisms by a business entity.

Money laundering in Malaysia is not a significant issue; however, its financial sectors are susceptible to crimes related to narcotics traffickers, financiers of terrorism and other criminal elements.

Various reports show that since 2000, Malaysia has made significant progress in constructing a comprehensive AML regime. Malaysia's AMLATF requires all reporting institutions to create ongoing employee training programs to guard against and recognize suspicious transactions. Institutions must also require training for subsidiaries outside of Malaysia.

In 2010, Financial Action Task Force (FATF) President, Luis Urrutia Corral cited Malaysia as being a country with a well-developed AML/CFT framework. However, improving AML/CFT compliance and enforcement is an ongoing process. I strongly felt that Malaysia can't rest on its laurels.

Thus, in terms of a compliance program, we hope that all six steps outlined by the BNM guide will be followed and applied by member firms fully and strictly. The steps are:

- i. Member firms are required to co-operate and work with BNM as the competent authority under the AMLATF and other authorities with regards to all anti-money laundering and anti-terrorism financing measures;
- ii. Members and member firms that provide the relevant services have to comply with the AMLATF;
- iii. Internal policies with respect to anti-money laundering need to be established and implemented in every member firm;
- iv. Each member and member firm need to develop audit functions to evaluate policies, procedures and controls to test compliance with the measures taken to comply with the provisions of the AMLATF and the effectiveness of such measures;
- v. On-going review and updating of policies and practices are required by each member and member firm; and
- vi. Obligation on officers of a member or member firm to take all reasonable steps to ensure compliance with the obligations under Part IV of the AMLATF.


AT: What is your vision for anti-corruption development in Malaysia in the near future?

TSAK: MACC's achievements and success throughout 2009–2013 is testament to the fact that the commission is heading in the right direction. Last year, we witnessed the implementation of various transformation initiatives. The MACC is also continuously increasing efforts in improving the quality of public education in corruption prevention. There is also a need to increase streamline public education that will generate the passion to abhor corruption and develop a society with integrity. A holistic approach is required without considering race, religion, age and political ideology. The focus of the education in the prevention of corruption will also be tuned toward the student population, as well as the nation's youth in the hope that they will be the torchbearers of a nation in leading it with the highest integrity.

Since assuming leadership of the MACC, I have witnessed immense challenges as well as obstacles faced by the MACC in fulfilling its core duties and responsibilities in eradicating corruption in the country. The MACC will continue to fight corruption with the highest level of commitment together with the aspiration of the public joining us in unison in curbing and ultimately eradicating the hideous act of corruption.

AT: How can implementation of such a vision be coordinated with other government institutions to formulate a comprehensive framework and system to detect and prevent financial crimes in Malaysia?

TSAK: We believe that in the MACC we can't detect and prevent financial crimes alone. All parties from public and private sectors need to work together. We need a coordinated approach with the involvement of each government institution to tackle the problem or issue that we are facing today. We have a special task force which is headed by the attorney general, which is part of Malaysia's NCC. Malaysia has adopted a collaborative, multi-agency approach in implementing AML and combating the financing of terrorism program that is in keeping with international standards. Over the decade since the enactment of the 2001 AMLATF, Malaysia has established the NCC, which brings together policy and implementing ministries and agencies to ensure that Malaysia implements an effective national AML system. The NCC has set in place a national certified financial investigators program (CFIP), including a comprehensive training module for AML investigation processes and procedures, forensic accounting, and computer forensics. In 2009, BNM launched the three-year National AML/CFT Strategic Plan, which focused on coordinating implementation, enhancing the legal framework, improving institutional framework and capacity building. Just as NCC is comprised of 16 agencies including RMP, BNM and Attorney General Chambers we should have a coordinated vision in combating corruption, money laundering and financial crime to create a healthy democratic society.

As we can see from FATF's latest report, building up an appropriate and balanced AML regime based on domestic circumstances requires extensive coordination among competent authorities and between public authorities and the private sector. Thus, effective information exchange between the public and private sectors will form an integral part of a country's strategy for combating money laundering and terrorist financing while promoting financial inclusion. 

Interviewed by: Hue Dang, CAMS, head of Asia, ACAMS, Hong Kong, China, hdang@acams.org



Cathy Murray

Sales Department

Cathy Murray serves as the account manager for Canada and the Mid-Atlantic region for ACAMS. She has been with the organization for three years and looks forward to many more.

Murray has been in sales for 20 years and prior to joining ACAMS, she worked for various institutions in the sales department where she consistently met sales goals and objectives. In addition, Murray has volunteered for charitable organizations that focus on offering care for the poor and homeless.

Since joining ACAMS, Murray has attended three conferences, including the Canada Inaugural Conference where she had the opportunity to interact with her customers face-to-face and learn more about the needs of compliance professionals.

Murray has had the opportunity to travel to Europe, South America, Central America, the Caribbean, Canada and all over the U.S.

ACAMS Today: What is the best part of your job?

Cathy Murray: Being part of an organization that is committed to excellence in AML/CTF training and education. It imparts a certain amount of pride in me to be able to speak with my customers and know that I will be able to provide them with access to the training and education that will allow them to excel at their jobs. I really enjoy interacting with my customers, taking the time to really listen to their specific needs and being

able to provide them with the tools that will fulfill those needs. My customers' needs are specific to their region, organization type and position within the organization.

AT: You are the account representative for Mid-Atlantic United States and Canada. Where do you see the membership in these regions in five years?

CM: I believe that ACAMS membership will continue to grow in the Mid-Atlantic due to its established reputation within AML community and because of ACAMS dedication to maintaining a high level of training. ACAMS membership in Canada continues to grow at a rapid pace in part because of the added exposure in the region including the *Inaugural Canada Conference* in Toronto last year as well as the upcoming *2nd Annual Canada Conference*. The high level of education and training that ACAMS provides will continue to fuel growth throughout the Mid-Atlantic and Canada as more organizations increase focus on training and education for existing employees and new hires.

AT: You speak with compliance professionals every day, what have you found that inspires compliance professionals to keep fighting financial crime on a daily basis?

CM: Pride, dedication and enthusiasm are what come to mind when I think of the average person that takes on an AML/CTF role. AML professionals are the frontline that protects their organizations and the public from all types of criminal activity. What I

see with my customers is that they are very committed to staying educated and informed about the AML climate as a whole as well as to what is specific to their region, organization type, etc.

AT: Out of all the ACAMS conferences you have attended, which one was your most memorable and why?

CM: The *18th Annual International AML and Financial Crime Conference* and the *Canada Inaugural Conference*. This was the first time I was able to actually connect with many of the people I had been speaking to for a long time and in both cases a great opportunity to have that one-on-one face time that is so invaluable.

AT: What is your favorite book and which book are you currently reading?

CM: I am actually rereading *100 Years of Solitude* which I love and I am getting started with *After the Music Stopped*, which is about the financial meltdown of 2008. I do not have a type of book I favor over another. Reading is my escape and I think that you can take some piece of knowledge away from any book. It does not have to be a great work of art it can be a great short story that captures your imagination. **TA**

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

Master of Anti-Money Laundering and Counter Terrorist Financing

Charles Sturt University (CSU), in partnership with the Association of Certified Anti-Money Laundering Specialists (ACAMS), offers postgraduate programs that provide specialist anti-money laundering and counter terrorist financing education that will develop the knowledge and skills required to advance your career.

The Master of Anti-Money Laundering and Counter Terrorist Financing (AML-CTF) is the only postgraduate program of its kind being taught at an International university.

The course was developed in consultation with law enforcement, financial regulators, and government agencies with significant input from the finance, banking and corporate sectors in Australia, North America, Europe, Middle East and Asia-Pacific.

This graduate program is delivered by CSU's Australian Graduate School of Policing and Security and incorporates the CAMS certification as an integral part of the coursework required to successfully complete the program. Part-time students can complete the Graduate Certificate in one year, the Graduate Diploma in two years and the Master's degree in three years.

The course is designed to promote best practice in AML-CTF investigation, compliance, prevention and management in the private and public sectors. Subjects are taught via online distance education with interactive sessions and lectures provided by academic, law, criminal justice and industry experts in the AML-CTF field.

MARCH, JULY AND NOVEMBER 2014 REGISTRATION

Enrollment for the March 2014 session is now available. For further information please visit www.csu.edu.au/aml or phone: +61 (2) 993 25207 or +61 (2) 993 25212.

Those who complete the Master Degree through this educational partnership:

- Earn the Certified Anti-Money Laundering Specialist (CAMS) Certification, or if already certified, advanced standing and subject credits in the Master's program.
- Obtain the tools and educational resources to competitively position themselves.
- Contribute to establishing best practices in field, making a lasting impression on the industry.

STUDY MODE

Distance education

WHEN

Session 1 (March)

Session 2 (July)

Session 3 (Nov)

DURATION

Graduate Certificate: 1 year part-time

Graduate Diploma: 2 years part-time

Master: 3 years part-time

APPLY NOW

http://www.csu.edu.au/courses/postgraduate/counter_terrorist_financing/apply-now

Fine Prevention Tools

Banks and corporations all over the world rely on Alacra Compliance Solutions to onboard customers efficiently and reduce regulatory, financial and reputational risk.

We apply a consistent process to CIP, KYC, EDD, client onboarding and credit investigations. Our tools simultaneously search across web and premium databases and deliver an investigation results report and audit trail on every onboarding case.

Streamline workflow, improve productivity and meet regulatory requirements.



Contact Us

AMERICAS (HQ)

100 Broadway, Suite 1101
New York, New York 10005
United States
T +1 (212) 363-9620
F +1 (212) 363-9630
E info@alacra.com

EMEA & APAC

125 Old Broad Street, 6th Floor
London EC2N 1AR
United Kingdom
T +44 (0) 20 3059 5765
F +44 (0) 20 3192 5577
alacra.com/compliance-solutions