

# ACAMS<sup>®</sup> TODAY

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

## Viewing in monochrome? 46



MARCH-MAY 2011  
VOL. 10 NO. 2

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

[www.ACAMS.org](http://www.ACAMS.org)  
[www.ACAMS.org/espanol](http://www.ACAMS.org/espanol)

Inside the white-  
collar criminal mind 20

# PATRIOT OFFICER®

**#1 BSA/AML/ATF/FACTA/UGEA/ANTI-FRAUD**

Consolidate AML/FRAUD on One Centralized Case Management Platform  
with Maximum Efficiency

Endorsed By The Largest Bankers Associations and Has Passed Examinations

**“THOUSANDS OF TIMES”**

Financial  
Intelligence  
Center



Compliance  
Network  
UCEN.net



## GlobalVision Systems, Inc.

9301 Oakdale Avenue, Suite 100, Chatsworth, CA 91311

Phone: (818) 998-7851 Email: [sales@gv-systems.com](mailto:sales@gv-systems.com)

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

**SAS® for Banking**

Credit Risk Management | Credit Scoring | Fair Banking | Fraud Management | Anti-Money Laundering  
Market Risk Management | Operational Risk Management



**What if you could join the 33% of financial institutions poised to come out of this economic crisis stronger and more resilient?**

**You can. SAS gives you The Power to Know.®**

**SAS software is used by more than 3,100 financial institutions worldwide, including 96% of banks in the FORTUNE Global 500.®**

▶▶ [www.sas.com/resilient](http://www.sas.com/resilient)  
for a free special report



**THE  
POWER  
TO KNOW.**

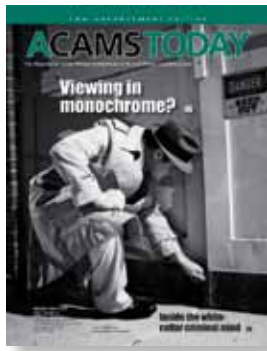


Association of Certified  
Anti-Money Laundering  
Specialists®

ACAMS®

# ACAMSTODAY

## ON THE COVER



Viewing in  
monochrome?

46

Cover photo: Kaitlin Racine

*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](mailto:info@acams.org)  
Web site: [www.ACAMS.org](http://www.ACAMS.org)  
[www.ACAMS.org/espanol](http://www.ACAMS.org/espanol)

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

## ACAMS

<b>Executive Vice President</b>	John J. Byrne, CAMS
<b>Editor/Communications Manager</b>	Karla Monterrosa-Yancey, CAMS
<b>Global Director of Conferences and Training</b>	Eva Bender
<b>Senior Vice President of Business Development</b>	Geoffrey Chunowitz, CAMS
<b>Head of Asia</b>	Hue Dang, CAMS
<b>Director of Operations for Latin America</b>	Gonzalo Vila, CAMS
<b>Director of Marketing</b>	Kourtney McCarty Llopis
<b>Certification Manager</b>	Giovanna Oquendo Llano, CAMS
<b>Account Executives</b>	David Kehr, Sonia Leon and Jose Lewis
<b>Corporate Sponsorship and Advertising</b>	Andrea Winter
<b>Graphic Design</b>	Victoria Racine

## ACAMS ADVISORY BOARD

<b>Chairman:</b> <b>Richard A. Small, CAMS</b> Enterprise Wide AML and Sanctions Risk Management, American Express, USA	<b>William J. Fox</b> Senior Vice President, Global AML and Economic Sanctions Executive Bank of America, Charlotte, NC, USA	<b>Anthony Luis Rodriguez, CAMS, CPA</b> Chief Global Compliance Officer, RIA Financial Services, Cerritos, CA, USA
<b>Samar Baasiri, CAMS</b> Head of Compliance Unit, BankMed, Lebanon	<b>Susan Galli, CAMS</b> Director of AML Programs, HSBC Holdings North America, Inc, New York, NY, USA	<b>Nancy Saur, CAMS, FICA</b> Regional Head of Compliance & Risk Management, ATC Group N.V., Cayman Islands
<b>David Clark, CAMS</b> Head of Intelligence and Analysis for Barclays Wealth Financial Crime, Barclays Wealth Financial Crime, UK	<b>Peter Hazlewood</b> Managing Director Compliance Services & Security Group Legal, Compliance, Secretariat and Security, DBS Bank, Hong Kong	<b>Markus E. Schulz</b> Chief Compliance Officer Global Life & Banking, Zurich Insurance Company Ltd, Zurich, Switzerland
<b>Brian L. Ferrell</b> Assistant Vice President and Assistant General Counsel of AML/OFAC/FCPA Compliance, The Hartford Financial Services Group, Inc., USA	<b>Michael Kelsey, CAMS</b> Global AML Compliance Officer, TD Bank North, MT Laurel, NJ, USA	<b>Daniel Soto, CAMS</b> Executive Compliance Director and BSA/AML Officer, Charlotte, NC, USA
	<b>William D. Langford</b> Senior Vice President and Director of Global AML, JP Morgan Chase and Co., New York, NY, USA	



- 6** From the editor
- 6** November–January CAMS Graduates
- 8** Member spotlights
- 9** A message from the Executive Vice President
- 10** Expert spotlights
- 14** A guide for law enforcement and financial institutions: AML and risk challenges facing financial institutions issuing prepaid cards
- 18** Homegrown risk: The growing threat of insider fraud
- 20** Inside the white-collar criminal mind (Predictive forecasting or palm reading)
- 24** Organized crime at your doorstep  
Lessons learned from prosecuting organized fraud rings
- 28** Human trafficking: AML’s dilemma
- 32** The prepaid card — Growing in use and risk
- 34** Tackling the AML compliance challenges of emerging payment alternatives: Follow the yellow (gold) brick road into digital currencies
- 38** When to make the call to law enforcement
- 40** Before – and After – You Start Talking to Law Enforcement  
Important tips from the lawyers
- 42** Suspicious Activity Reporting:  
Quality assurance is key to maximizing reporting value
- 44** Federal Register  
–The daily journal of the U.S. government
- 46** Viewing in monochrome?
- 50** AML risk assessments
- 54** Demystifying the wire transfer for investigators
- 58** Foreign direct investments and money laundering trends
- 62** Napoleon’s legacy:  
How 19th century thinking skews AML in the 21st century
- 64** Combating trade-based money laundering through global partnerships
- 68** The Foreign Account Tax Compliance Act:  
Stay tuned to see its effects
- 72** Know Your Chapter
- 79** Meet the ACAMS staff



Some of my favorite TV shows involve cops, detectives and investigators. Lately, I have been watching *Hawaii Five-O*, *Castle*, *White Collar* and the *Mentalist*. I always wonder what makes cop and detective shows so appealing to mainstream society. For the vast majority of people the closest they come to directly interacting or walking in the steps of a law enforcement official is a Thursday night on the couch watching their favorite cop show. However, for those in the AML field interacting with law enforcement is part of the routine. Compliance and law enforcement professionals work side-by-side in the fight against crime. We created this special edition of *ACAMS Today* to highlight the joint efforts of both professionals, with the goal of helping compliance and law enforcement professionals form successful partnerships.

The lead article *Viewing in monochrome?* articulates the importance of understanding the different perspectives between compliance and law enforcement. Learn the importance of partnerships and how innovations can champion the efforts of compliance and law enforcement professionals in combating crime.

Have you ever wondered what goes on inside a criminal mind? *Inside the white-collar criminal mind* gives a sneak peek at the cryptic world of a criminal. Discover the immoral qualities that might help you find a white-collar criminal within your organization.

We are constantly making decisions everyday of our lives. The article *When to make the call to law enforcement* offers guidelines on how to make the appropriate decision. Learn what experts have to say about when you should make that important call.

Criminals try to constantly exploit every angle. The article *Organized crime at your doorstep* outlines what four areas every institution should be mindful of. Criminals depend on their understanding of human nature when trying to take advantage of your institution.

Ascertain the importance of quality reporting in *Suspicious Activity Reporting: Quality assurance is key to maximizing reporting value*. The article outlines how to obtain SAR quality by following the five "W's." Remember that a poorly prepared SAR could negatively impact law enforcement's efforts in an investigation.

As AML professionals we may never be able to say "Book 'em Danno" but working closely with law enforcement will help us all contribute to minimizing crime.

Also, we would like to thank our many authors that contribute to the *ACAMS Today* and as such we would like you, the readers to nominate an article from 2010 that you enjoyed or found the most useful for the *ACAMS Today* Article of the Year Award. Please indicate the article title, author, in which edition it was printed and a brief summary to support your nomination. All nominations must be received by August 1, 2011. Also, please send all nominations to [editor@acams.org](mailto:editor@acams.org). The winner will receive their award at the Annual ACAMS Conference in Las Vegas, Nevada in September.

As always do not forget to send your comments, ideas for articles and submissions directly to me at [editor@acams.org](mailto:editor@acams.org). 

Karla Monterrosa-Yancey, CAMS  
editor/communications manager  
ACAMS

## November–January CAMS Graduates

Sameh Abozina  
Bonnielyn Adderley  
Amjad Al-Shawahneh  
Dana Aldridge  
Asim Ali  
Gary Almiron  
Nasir Ameen  
Stephanie Anstead  
Roxanne Arambula  
Anne Archer  
Eric Arciniega  
Pembe Arifoglu  
Christopher Armstrong  
David Arroyo  
Andria Arsic  
Emre Atabay  
Lisa Austin  
Donna Baer  
Craig Bailey  
Timothy Baker  
Amrit Bansal  
Zhou Baokang  
Henry Barhan  
Kevin Benes  
Zheng Benju  
Thomas Bennington  
Amit Bhojwani  
Susan Bnoit  
Zhou Bo  
Adrian Bock  
Ricky Boirard  
Maud Bokkweink  
Olga Bolet  
Leonard Bolton  
Kelvin Bonilla  
Sujata Bose  
John Bower  
Rendell Briggs  
Andrew Brinker  
Sterling Broadbent  
Charles Brown  
Michael Brunt  
Ann Bu  
Melissa Burrow  
David Burton  
Vefa Buyukalpelli  
Augusto Cabrera  
Ronan Caffrey  
William Caldeira  
Emilio Cardenas  
Tammy Carroll  
Adriana Castano  
Sevgi Cayonlu  
Jeff Chamberlain  
Dominic Chan  
Michelle Ching Yuen Chan  
Colin Chapman  
Jose Chavez Sanchez  
Soon Chye Cheah



## CAMS GRADUATES

Xin Yuan Chen  
May Cheong  
Vadym Chernysh  
Raluca Chiciu  
Patricia Chin  
Joseph Chin-sang  
Devika Chopra  
Clement Chu  
Celine Chua  
Kevin Chua  
Tracy Laine Cisco  
Clarissa Cluriel  
David Conrad  
Anca Constantin  
Stephanie Cook  
Francois Cooke  
Melonie Coombs  
Tracey Cooper  
Karen Cordon  
Melissa Cram-Stentz  
Sergio Crivorot  
Brian Curtis  
Chandramohan D  
Li Dai  
Gao Dalan  
Marlon Dalrymple  
He Dan  
Liu Dan  
Shi Dan  
Michael de Armas  
Carla De Martino  
Aline de Oliveira  
Christian Decker  
Michelle Delk  
Kevin Delli-Colli  
Ling Deng  
Eileen Derzsi  
Steven DeTomaso  
Leslie Devereaux  
Susan Devlin  
Aboubacar Dicko  
David Dinkins  
John Duffy  
Michael Eisner  
Oliver Elam  
Jayson Ensign  
Derya Erbay  
Antonina Esguerra  
Yesenia Espinal  
Bertila Espino  
Anna Estrada  
Andrea Eturriaga  
Charles Everson  
Yang Fan  
Jin Fang  
Tracie Farias  
Maria Farias Molina  
Christine Feldpausch  
Michael Fitzsimmons  
Donna Fong

Teo Kah Fook  
David Foster  
Richard Foster  
Sylvia Fung  
Autumn G.Morton  
Curtis Galera  
Melek Galip  
Srinivasan Ganesan  
Javier Garaeta  
Gabriela Garcia  
Marlene Gardner  
Mariem Garrido  
James Garrison  
Armen Gemdjan  
Huda Ghaith  
Dominique Gilio-Chaffin  
Karen Goebert  
Minyang Goh  
Patricia Golding  
Karianne Golemme  
Stephanie Gonzalez  
Douglas Gorenflo  
K.R. Gracious Raj  
Edward Graf  
Chris Grippa  
Nancy Gross  
Hale Halasy  
Fahad Hameed  
Marzouk Hammouda  
Chad Harkey  
Mona Hayes  
Patrick Hayes  
Frances Hedgepeth  
Karla Hernandez  
Herlin Herrera  
Phillip Hetherington  
Ryan Hodge  
Thomas Holland  
Louis Howell  
Jen-Chieh Huang  
Richard Huits  
James Hunt  
Kathryn Hunt  
Ellen Huntzinger  
Dwi Indrawan  
Ashley Ivan  
Jesse Jacoby  
Qu Jianyu  
Shen Jianzhong  
He Jifeng  
Tao Jin  
Feng Jing  
Han Jingjing  
Jasmin Jochum  
Dawana Johnson  
John Johnson  
Lourdes Johnson  
Sara Johnson  
Shaq Johnson  
Nikki Jones

Bart Jonker  
Vincent Jordan  
Zhou Jun  
Rashi Juneja  
Danny Kaleita  
Koichi Kamata  
Sifa Karahasanoglu  
Choukri Kassisse  
Miriam Kavanagh  
Tatyana Kazak  
Anochie Kelechi  
Donald Kelsey  
Johnny Kemp  
Iain Kenny  
Huda Khatreja  
Bheki Khumalo  
David Kilonzi  
Hee Kim  
Gregory Kimball  
Maxim Kiselev  
Paul Klemcke  
Kristine Klitzke  
Maciej Kolodziej  
John Kovacs  
Nadezhda Kozyreva  
Kalyanaraman Krishbasamy  
Dmitry Krupyshev  
Li Kun  
Pui Yi Kwan  
Sharon Lahr  
Jiang Lan  
Edwin Langmer  
Elena Lasa  
John Lash  
Sergio Latelier  
Jennifer Lay  
Rachel Layburn  
Jennifer Leach  
Kit Leary  
Kim Leman  
Lee Leong  
Yin Kwan Leong  
Clara Leung  
Anthony Leveille  
Thomas Leysath  
Que Li  
Zalman Liberman  
Jennifer Lin  
Armando Linares  
Vanina Lombardi Rodriguez  
Cristina Loomis  
Zhang Lu  
Judith Mack  
Brian Maguire  
Alex Mahdavi  
Amer Mahmoud  
Jayaprakash Mangalore  
George Martin  
Suella Matthews  
Tawaya Mauldin

Amy McCann  
Leo McCormick  
Trina McGhie  
Yolanda Coley McNair  
Jiang Mei  
Keith Merritt  
Ismail Mert  
Kelvin Miller  
Sarah Miller  
Chen Ming  
Christine Mingie  
Terry Mipro  
Amy Misok  
Bryan Mizeur  
Hanifa Mohamed  
Sundeep Mohan  
Abdul Moin  
David Monegro  
Junior Moore  
Victoria Moore  
Engrisel Munoz  
Ismael Munoz Olivera  
Munzer Nabhan  
Pinder Nahal  
Adersh Nair  
Cathy Nanos  
Tania Narciso  
Reiko Narita  
Royston Ng  
Sherman Ng  
Susann Ng  
Angela Nightingale  
Andrea Novosedlikova  
Mariel Nunez Arzuaga  
Phillip O'Connell  
Jeanette O'Rourke  
Matthew O'Toole  
Ifeanyi Onwukwe  
Obafemi Oyenuga  
Huseyin Ozarin  
Nevzat Ozkunt  
Ahmet Murat Ozsan  
Hasan Ozyel  
Paula Paldino  
Ajay Panandikar  
Eun Park  
Bryan Parker  
Deborah Parker  
Nidhi Patel  
Joan Pendleton  
Li Peng  
Juan Peñuala-Velez  
Orlando Pereira de Lima Neto  
José Pero-Sanz  
Kathleen Peters  
Dania Pfeiffer  
Obiang Philippe  
Kenneth Piana  
Rosanna Piccolo

Bhanu Prabhat  
Nancy Price  
Nick Pritchard  
Xian Zhong Qiao  
Yan Qiu  
Troy Rabenseting  
Athmananda Rai  
Arati Rava  
Camille Remus  
Brunilda Reyes  
Marcia Rickenbacker  
Syed Rizvi  
Lynn Robbins  
Linda Robertsom  
Shanica Robin  
Christene Robinson  
Stephen Robinson  
Carmen Rodriguez  
Miguel Rodriguez  
Georgiana Roman  
Julie Roper  
George Rose  
Jonathan Rose  
Anita Rueda  
Harold Rutherford  
Nie Sa  
Eric Saltzman  
Eira Sanchez  
Marcelo Sandoval Trancoso  
Tina Sarnoff  
Dione Schick  
Debra Schnell  
Stephen Schwartz  
Kenneth Schwein  
Joaquín Scocozza Martinez  
Richard Seely  
Chetan Sehgal  
Joe Seratte  
Sudhir Sharma  
Vinay Sharma  
Karichery Shasheendran  
Mohamad Shbaro  
Barbara Shore  
Matt Shull  
Zhao Shuyun  
Ajit Singh  
Michael Skelly  
Yvonne Smith  
Kimberly Sokolowski  
Yakov Sosonov  
Lukas St. Clair  
Elizabeth Stanley  
Natalie Stark  
Alyssa Stellmaker  
Joan Stewart  
Stephen Gunawan Suryo  
Ann Swain  
Shawn Swartout

William Tanem  
Adwait A. Tare  
Bengu Tasci  
Salameh Tayen  
Cizge Tekeli  
Basak Tekerek  
Basak Tekerek  
Jean Thaler  
Deborah Tourloukis  
James Trejo  
Anna Tsai  
Hikmet Turkman  
Hikmet Turkmen  
Oscar Urcuyo  
Adnan Usmani  
William Valentine  
Joan Van Lieshout  
Maria Velegris  
Olivia Vernier  
Shirley Vickery  
Irma Villalobos  
Donald Wagner  
Susan Wahba  
Swapnil Walimbe  
Linda Walker  
Brenda Wallace  
Colin Waller  
Michael Webb  
Liza Webber  
Zhao Weiping  
Chen Wen  
Wu Wenfang  
Sanja Whitman  
Slamet Widodo  
John Williams  
Jennifer Wills  
Barbara Wojtyniak  
Angeline Wong  
Audrey Wong  
Eileen Wong  
Julie Wong  
Sue Wong  
Sharon Yan Xiaolong  
Ye Xiaoting  
Anna Yalkut  
Song Yang  
Yi Yang  
Julia Yao  
Wang Yeqing  
Sean Yi  
Yuan Yin  
Ilkin Yogurtcuoglu  
Xu Yongping  
Lynn Yaping Yu  
Zandra Yuen  
Arbab zafar  
Marcin Zdrojowy  
Dai Zhisong  
Michael Zytnick



## MEMBER SPOTLIGHT



Karim Rajwani, B.A., C.A.,  
CAMS  
Toronto, ON Canada

Mr. Rajwani is currently the chief anti-money laundering officer for RBC Financial Group (RBC). He is responsible for leading RBC's Global AML program, which encompasses anti-money laundering, anti-terrorism, economic sanctions, anti-bribery anti-corruption, and client risk management initiatives. Drawing on more than 20 years of risk management, compliance and financial accounting experience, Rajwani is a leading authority on anti-money laundering and counter-terrorist financing matters both domestically and internationally and speaks frequently on these matters in banking, legal, compliance and academic platforms.

Rajwani is co-chair of the ACAMS Canada Chapter and is also an appointed member of the Advisory Council on National Security to the Office of the Prime Minister of Canada on issues of national security.

Rajwani has overseen the development and implementation of RBC's AML/CTF program from its inception. As chief anti-money laundering officer of Canada's largest bank, Rajwani's has led RBC's development and implementation of numerous AML solutions covering offices in 53 countries and clients

across retail banking, wealth management, insurance, corporate and investment banking platforms.

Prior to taking on his current role with RBC, Rajwani held various management positions focused on risk management, internal controls, operational risk and IT development. In addition to his risk management experience, Rajwani has worked for various Financial Institutions, Chartered Accounting and Management Consulting firms overseeing the implementation of enterprise-wide risk management and compliance initiatives.

Rajwani has a double honors degree in Accounting and Finance and is a member of the Institute of Chartered Accountants in Canada, England and Wales.




David M. Schiffer  
Mineola, New York

David Schiffer is the founder and president of Safe Banking Systems (SBS), a provider of AML and compliance solutions with headquarters in Mineola, NY. For over a decade, Schiffer has directed his company's efforts to combat money laundering, terrorist financing, fraud and other criminal activity by providing banks, non-bank financial institu-

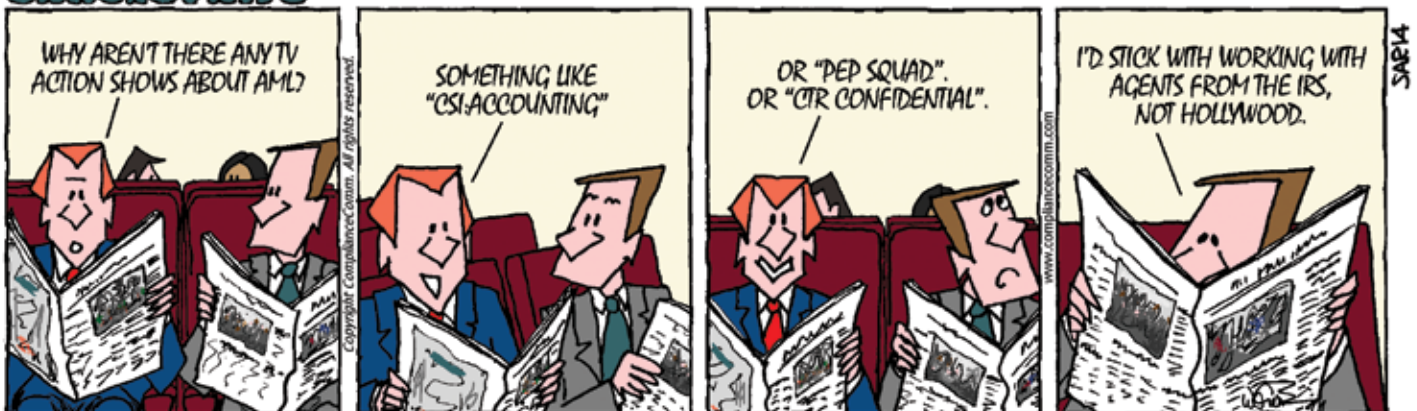
tions and corporations with the latest technology to fight financial crime and find the "bad guys."

Schiffer's support of ACAMS dates back to its inception when Safe Banking Systems became ACAMS' first ever service member. His son Mark, a principal of the company, was awarded the CAMS designation as a member of the first class to be certified. SBS is proud of its history with the ACAMS organization as an event sponsor and contributor to *ACAMS Today*. Schiffer has authored two articles, *The PEPs Challenge* and *Homegrown Risk*.

Schiffer believes that the role of SBS is not only to provide innovative solutions to clients but to also share practical knowledge and experience. He has met with the chief counsels and their investigative teams at both the U.S. Senate Commerce Committee and U.S. House Committee on Homeland Security and has been interviewed by several radio stations.

Prior to founding SBS, Schiffer ran other technology companies and also taught in the New York City school system. A native New Yorker, Schiffer received his M.S. in Computer Science from SUNY Stony Brook, his M.A. in Mathematics from Hunter College, NY and his undergraduate degree, a B.S. in Mathematics also from SUNY Stony Brook, NY. In August 2010, Schiffer was honored by the American Kidney Fund for his charitable support of their organization. 

### SARSENSTRIPS™



Produced by ComplianceComm





# A great way to stay connected

**W**e are extremely proud to publish this “Special Law Enforcement Edition” of *ACAMS Today*. I know you will find it as valuable as I do, to focus entirely on the men and women of law enforcement, who are community’s front line against criminals throughout the world.

When I joined ACAMS last February, I was committed to recognizing the important role law enforcement plays in our organization and in the global efforts to combat money laundering, financial crime and all other related efforts that have a monetary component. In the past year, we have met with state, federal and international law enforcement representatives on improving our training, and overall general awareness of the global AML community on the importance of working closely with our allies from law enforcement. You can expect to see more training from ACAMS on investigations, responding to law enforcement requests for information and how to prepare quality SARs or STRs. Law enforcement agencies are true partners of the AML professional private sector and we need to do our part to assist them.

Please give us feedback on this effort and ideas for themes for future editions.

## ACAMS Chapters — A great way to stay connected

We had a 50 percent increase in ACAMS chapters in 2010. Look for new chapters in Florida, the Midwest, North East and West Coast of the United States. Chapters will also be created in Europe, Asia, Latin America and the Middle East. So, growth is continuing in 2011, and with the recommendations being developed by a Steering Committee created in December, chapters will indeed be a major way for our members to stay engaged with one another.

I have been fortunate to be able to travel to a number of chapter launches and am truly impressed by the professionalism exhibited by the board members. Their commitment to encouraging feedback and participation

should ensure active and connected ACAMS members for a long time to come.

It is essential that our chapter boards continue to be composed of a vast array of AML professionals from the government, the consulting area and the financial industry. Keep in mind as you consider creating a chapter in your area, the more diversity in your board, the more value you will be able to provide to local ACAMS members.

It is essential that our chapter boards continue to be composed of a vast array of AML professionals

## The CAMS Examination — An assessment of the AML professional like no other

Another area of critical importance to employers in both the private and public sector is whether an AML professional candidate is truly prepared for the challenges of this industry. I have been fortunate to have been in this community for a very long time (no jokes please!) and it is clear to me that the CAMS exam is the only true testing measure of AML understanding. There is no valid competition to our process and we have just updated the examination in 2011 to reflect changes in laws, regulations and AML-related coverage. Our exam is also psychometrically reviewed and is not an “open-book” examination. We also do not “grandfather” anyone! So, the next time you are contacted by the competition, remember, there is no competition. Be

proud of your CAMS designation and share stories with us on how that credential has helped you in your career.

## Task Force activity — Another vehicle for participation

ACAMS has made a strategic decision to revise all of our existing task forces and to create several new groups. We feel strongly that the expansion of task forces, chapters and other committees will create ample opportunities for members to stay involved with the ACAMS community.


In some cases, ACAMS members who have long served with distinction, are no longer on several of our standing task forces, as we have added new members or individuals that have been members but never participated in an active role. This approach may seem harsh but it should not be seen that way.

For conference planning and training advice, it is important that ACAMS hear from new members of our diverse community — whether it is from MSBs, insurance, securities, casinos or others from the AML consulting community. We believe these changes will pay immediate benefits.

I am convinced that the dedicated ACAMS member will find a way to stay involved and we welcome that support.

To get you to start thinking about new or revitalized participation, let us know your interest in any of the following task forces:

- Sanctions
- Human Trafficking
- Securities
- Insurance
- Financial Intelligence Units (FIUs)
- Latin America
- Caribbean

Finally, if you have an idea for another task force, let us know. 

John J. Byrne, CAMS  
ACAMS executive vice president

# Simon Dilloway: Follow the money trail



**A** *CAMS Today* had the opportunity to speak with Simon Dilloway, founder of Lopham Consultancy.

Dilloway spent over 30 years in the Metropolitan Police in London. He specialized in the investigation of corruption, financial crime and terrorist financing by the use of financial investigation methods and collection and analysis of financial intelligence. Whilst leading a team in the Special Branch National Terrorist Financial Investigation Unit (NTFIU) at New Scotland Yard he used these techniques to great effect in the aftermath of the London bomb

attacks of 2005. He subsequently led the financial investigation and intelligence gathering operation that led to the arrest and conviction of the terrorists involved in the conspiracy to bring down seven airliners en route to North America. Since retiring from the police and founding Lopham Consultancy, he has assisted the European Commission, Council of Europe and United Nations Office on Drugs & Crime in capacity building missions around the globe. His training on AML and in particular CTF has been well received by law enforcement personnel from Russia, the Balkans, the

Middle East (including Iraq) and North Africa, as well as the UK, where he is an associate financial crime trainer with the NPIA. He has spoken at many international conferences, and recently presented on terrorist finance to the NATO Task Force Committee in Brussels. He is currently engaged in re-writing the national anti-money investigation and prosecution handbooks for the Republic of Vietnam.

He has a BSc(Hons) in Police Studies, and an MSc in Criminal Justice. He is a member of ACAMS, the Institute of Directors, and a Director & Fellow of the UK Security Institute.

**ACAMS Today:** Describe your current position and responsibilities?

**Simon Dilloway:** I have my own business which includes several companies. My main work at the moment is AML training and giving advice to the international public sector law enforcement. Also, I have just come back from training visits to Russia and Ukraine, and I am in the middle of rewriting the Vietnamese Handbook for ML investigators and prosecutors. In addition, I provide AML reviews and solutions to UK regulated companies, and have a third interest in an online e-learning and name checking site that is under development.

**AT:** How did you first become involved in law enforcement and the compliance field?

**SD:** I joined the Metropolitan Police in London in 1976, and served for almost 31 years. The latter part of that service was as a detective financial investigator, dealing with anti-corruption, drug trafficking, money laundering and ultimately, terrorism at the National Terrorist Financial Investigation Unit (NTFIU), then part of Special Branch at New Scotland Yard. After retirement in 2007, I started the companies mentioned above, and launched into my new career in the compliance field.

**AT:** What is the key to having a successful work relationship between law enforcement and compliance professionals?

**SD:** This is something that I was very much involved in while at the NTFIU. The key relationship has to be one of mutual trust — this is the most important thing. Clearly, those involved in compliance have legal obligations, both in disclosure and confidentiality, and on the other hand, law enforcement has to be careful not to reveal sensitive or classified information. If, however, both sides can go the extra mile to make the job easier for each other, we will at least be one-step closer to beating the bad guys.

**AT:** During your career you have been a part of many AML, TF and financial crime investigations, what commonalities have you found?

**SD:** An interesting question! Paradoxically, one of the common things is how different each investigation is. By that I mean that every time you investigate money laundering or terrorism, you find some new twist that

## Criminals are always developing new methods in the face of ongoing legislative improvements

you have not seen before, because criminals are always developing new methods in the face of ongoing legislative improvements. This is why I always preach the risk-based approach so passionately. It is the only way to avoid getting bogged down in set typologies, which itself leads to missing new methods of moving or disguising dirty money.

**AT:** How can those commonalities best be exploited by the compliance professional?

**SD:** The commonalities that are there need to be shared. This is an area where competition must be set aside, and the experiences of one institution should be broadcast to everyone else. This is of course promoted by many industry organizations — especially ACAMS. Ideally, firms should be in a position to use their AML expertise as a marketing tool, indicating to criminals, clients and the industry that they are a hard target. In addition, a well run AML regime also keeps a tighter control on other systems in the firm, thus improving governance all-round.

**AT:** What terrorist financing (TF) indicators should institutions be looking for and what advice do you have on how institutions can protect themselves against TF?

**SD:** As I have pointed out in previous articles, the nature of most TF is such that it can be very difficult to spot. The London bombers' finances, in hindsight, indicated very clearly what they were doing and why; however, that was only with the knowledge of what they subsequently did. The actual activity was no different to that of many other young men of the same demographic. Institutions should


be looking for transactions to or from countries known to be destinations, or transit points for TF. They should thoroughly check identity of clients, and be especially vigilant for any reluctance to provide supporting evidence of identity.

In truth, however, there is no foolproof method beyond what is done for AML. The important thing is ensuring that procedures are as tight as possible, and that record keeping and archiving are accurate and efficient, so that when law-enforcement comes calling, firms are able to supply top quality information quickly. That was the best help I could get as an investigator.

**AT:** How does following the money trail assist in breaching an AML or a TF case?

**SD:** To be able to connect the crime with the proceeds is the ultimate goal of an AML investigator. The whole purpose of a launderer's activity is to squirrel the money away through complicated layers of deals and transfers, and to protect the loot for later enjoyment — as we all know. If you can evidentially follow the money trail, not only do you identify where it is, but you get the chance to confiscate it. Also, when all the arcane and bizarre details of layering are put before a court as evidence, it actually strengthens the case and shows the launderer quite clearly as the crook!

**AT:** What is your proudest money laundering or terrorist financing bust?

**SD:** Aside from producing the costing and funding report for the London bombings of July 2005, the thing I am most proud of is leading the financial investigation into the plot to blow up airliners between London and North America. What started up as a small TF investigation to see me through to retirement from the police turned into the investigation of the biggest terrorist threat to face the UK. If this had been carried out successfully, potentially up to 4,000 people could have lost their lives, and I am immensely proud to have been part of the operation that prevented that. It also means that nowadays you will have trouble getting your toothpaste onto a flight, so I apologize for the inconvenience! 

*Interviewed by Karla Monterrosa-Yancey, CAMS, editor; ACAMS, editor@acams.org*

# David Olesky:

## Better lines of communication lead to better results

**A** *CAMS Today* caught up with Special Agent David Olesky for an informative interview. Special Agent Olesky has been with Drug Enforcement Administration (DEA) in excess of ten years. He has worked in the DEA New Jersey Division and DEA's Panama Country Office. Prior to joining DEA, GS Olesky worked for several years as an auditor for a public accounting firm where he obtained his CPA license.

**ACAMS Today:** Describe your current position and responsibilities?

**David Olesky:** I am a Special Agent Group Supervisor for DEA's Financial Investigations Group in Los Angeles. Our group focuses on the most significant drug traffickers operating in the Southwestern United States who are laundering drug proceeds both inside and outside of the financial system.

**AT:** How did you become involved with law enforcement and compliance?

**DO:** Prior to joining DEA, I had worked several years for a public Accounting Firm, obtained my CPA license, and then soon after applied to DEA. I have been with DEA just over ten years, and with my background in accounting, it was almost a natural fit that I would eventually find myself working in the Financial Investigations Group. This past year, I have interacted more with compliance officers as a result of the networking opportunities which have presented themselves via ACAMS. My group has a lot of interaction with financial institutions due to the nature of our group's mission.

**AT:** How can compliance professionals work more effectively with law enforcement?

**DO:** Do not be afraid to ask questions and interact with the agents and officers. When

your compliance office receives a subpoena request from law enforcement, feel free to contact the agent and discuss the request. Of course the investigators can not disclose anything that could potentially compromise the investigation; however, there is a practical middle-ground where both investigator and compliance officer can work optimally. Money laundering investigations tend to be complex, time consuming and may even last a number of months — if not years. It is best if both sides can establish a professional relationship so that both the investigator and the compliance officer understand the goals. For a DEA agent, even for me having worked in the financial arena, it can be very intimidating to take on a financial investigation. The majority of agents are more comfortable knocking down someone's door in the middle of the night then meeting with a compliance officer to discuss financial records. As a result, the better the lines of communication are between the two sides, the better the results will be as well.

**AT:** As a law enforcement professional, what are the three most important items you look for during a money laundering investigation?

**DO:** Number 1, we are looking for how the target subject first enters his drug proceeds into the financial system. Identifying the relationship between the specified unlawful activity or SUA and the entrance of the money into the financial system is critical. This is why knowing your customer (KYC) is very useful to the law enforcement community. Who and how the subject is first getting the proceeds into the system again are critical for us to identify. Number 2, we try to expand our investigations to the fullest and identify any and all associated accounts, assets, and individuals. And Number 3, we

try to track the flow of the money once it enters the system in hopes of identifying additional elements in the conspiracy and also potential forfeitures at the conclusion of the investigation.

**AT:** How can fellow law enforcement colleagues prepare to work effectively with financial institutions (FIs) during an investigation?

**DO:** Have a game plan and be specific in your requests to the financial institutions. That is where once again the lines of communication between the two parties are vital.

**AT:** What are the latest schemes you have seen in money laundering investigations and how can FIs prepare to combat these schemes?

**DO:** In June of 2010, the Mexican finance ministry published new regulations restricting dollar cash transactions at Mexican banks. The rule prohibits banks from receiving physical U.S. currency for transactions such as currency exchanges, deposits, payments of loans, or purchases of services including funds transfers, except below certain thresholds. For individuals who are customers, the aggregate limit in U.S. currency that a bank may receive from its customer per calendar month is only \$4,000. I believe these restrictions will have an impact on the flow of illegal drug proceeds (U.S. currency). There will continue to be an underground market in Mexico where U.S. currency is easily moved; however, I do believe that we will see more U.S. currency remaining within our borders and entering into the Financial System where previously it would have occurred South of our borders. Preliminary data I have seen in recent months has reflected that. I have also heard of reports of an increase in customer bank accounts across the U.S.-Mexican



border, this may be attributable to this change in regulations.

**AT:** Can you disclose general information about the latest cases you are working on?

**DO:** Our group tends to be focused on the Mexican drug cartels and the financial components associated with their drug trafficking. These groups are very savvy, and utilize a wide variety of methods to move their money — from basic bulk cash transportation of cash across the border to utilization of the Black Market Peso Exchange (BMPE). With the change in Mexican banking regulations I mentioned above, our group is trying to identify what alternatives these cartels are now using based upon the fact that it has become more difficult for them to enter into the Mexican Financial System. I think the U.S. compliance officers are going to have their hands full this year.

**AT:** What type of training should law enforcement professionals be receiving to work successfully with FIs or what type of training should FIs be receiving to work effectively with law enforcement?

## Do not be afraid to ask questions and interact with the agents and officers

**DO:** I mentioned previously the Black Market Peso Exchange. I think it would be wise for businesses to get an understanding of what it is and how it gets implemented. Whether you are in the business of selling computers, shoes, clothing, or widgets, any business could be subject to a Black Market Peso type scheme. I think it would be beneficial for compliance officers to receive training

on how businesses tend to structure these proceeds, what type of businesses typically are involved, and how to appropriately report suspect customers/businesses and also how to best document these situations in SARs. The better the SAR is written by the compliance officer, the more useful it becomes to the investigator.

**AT:** In your 10 years in the law enforcement field what are some of the most important lessons you have learned?

**DO:** One of the most important things I have learned is “trusting your instincts.” If something does not look right and your gut is telling you that something just does not fit, most likely it deserves to be given a second look. Trust those initial assessments, if you have been in the business long enough, whether for me in the drug trafficking arena or working within the financial system, trust your instincts and those of your people who are on the front lines for your business. **TA**

*Interviewed by Karla Monterrosa-Yancey, CAMS, editor; ACAMS, editor@acams.org*



## DO NOT LET OTHERS LAUNDER YOUR REPUTATION

**Sentinel Compliance & Risk** is a specialized solution for the prevention of money laundering that will help you to avoid legal, financial and reputation losses.

- Establish risk levels automatically individually for each of your customers.
- Monitor all channels and products.
- Generate behavioral profiles of each of your customers.
- Integrate and automatically update all your lists.
- Generate reports required by the Regulator.



[www.smartsoftint.com](http://www.smartsoftint.com) | [info@smartsoftint.com](mailto:info@smartsoftint.com)

A guide for law enforcement and financial institutions:

# AML and risk challenges facing financial institutions issuing prepaid cards



*Editor's note:*

*This is part one of a two part series.*

Whether used to provide cost-effective substitutes to traditional paper payments, such as government benefits, rebates and flexible savings accounts, or to provide a financial product to the under-banked or un-banked community, the prepaid card industry is rapidly growing both in the United States and internationally. According to research commissioned by MasterCard, Inc. and conducted by the Boston Consulting Group (BCG), the total value of the branded prepaid card opportunity in the U.S. is expected to surpass \$440 billion by 2017, nearly quadrupling its estimated value of \$120.2 billion in 2009. The study also shows the U.S. market will remain the largest branded prepaid segment in the world, holding 53 percent of the overall market share. India, the UK, Mexico, Italy, the Middle East and Brazil combined, will hold approximately 25 percent of the branded prepaid market by 2017. Brazil alone is expected to expand from \$1.7 billion in 2009 to more than \$17 billion in 2017.<sup>1</sup>

While most may be familiar with the prepaid card products that exist including gift, payroll and general purpose reloadable cards, do you have a good understanding what AML and risk controls financial institutions put into place before issuing or selling prepaid cards? The first part of this two-part series will address AML and risk considerations specifically for issuing financial institutions, followed by the second part which will focus on considerations for those companies wishing to market and sell prepaid card products. An examination of these subject areas provides law enforcement with a knowledge base for present and future investigations pertaining to prepaid cards.

At the end of the day,  
the issuer of the prepaid  
card is completely  
responsible for AML  
compliance on its products

For the most part, only financial institutions can be members of the card associations, meaning all prepaid cards are issued by a financial institution. If you look on the back of a prepaid card you will see the issuer statement. There are two routes financial institutions can take to issuing prepaid cards: (1) develop and issue a prepaid card program to market and sell directly to consumers themselves, or (2) assist third parties in developing prepaid card programs whereby the financial institution is the issuer but the third party is responsible to market and sell to consumers. This is typically referred to as a sponsorship model and is the model preferred by most financial institutions today. The third party is usually referred to as a "program manager" and the financial institution as the "issuer."

Financial institutions delving into the prepaid sponsorship industry, or indeed sponsorship of any bank products including credit cards and other lending products, need to place special emphasis on risk management of their third parties. In the past, "rent-a-charter" situations were troublesome to regulators and even though the industry has put substan-

tial controls in place to avoid this situation, regulators are again taking a hard look at financial institutions' third party risk management practices. In addition to contractual, operational and financial risk considerations, the issuer must consider its AML compliance obligations. At the end of the day, the issuer of the prepaid card is completely responsible for AML compliance on its products the same as any other bank product or service offered. The following are some specific considerations for financial institutions looking to issue prepaid cards.

#### Program manager due diligence

While the issuer is not offering a traditional commercial checking account to the program manager, it is providing access to financial products. The issuer should apply the same, if not more, customer identification program (CIP) and enhanced due diligence (EDD) standards to program managers as would apply to a traditional commercial account. This includes having complete information on the company and ownership structure, including background checks on the company itself and its beneficial owners. Financial statements, data security and disaster recovery policies are also recommended. A good third-party risk program will include a process for risk rating third parties, as well as standards for risk-based monitoring and periodic review of third party relationships. Refer to the regulatory agencies' web sites for further guidance on third party risk management.

#### AML and OFAC risk assessments

The issuer's enterprise-wide AML and OFAC Risk Assessments should encompass issuance of prepaid cards. Not only should the risk assessment include evaluation of the product, customer and geographic risks associated with the new business line, it should

<sup>1</sup>Payment News (2010), MasterCard Releases Prepaid Market Sizing Report, 12 July 2010, [www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html](http://www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html)

also include assessment of the risks associated with offering the products through third parties. The April 2010 FFIEC BSA/AML Examination Manual provides a good outline of the risk mitigation factors to consider.

### AML policy

In addition to ensuring that its enterprise-wide AML Program covers issuance of prepaid, the issuer should also have documented AML requirements to which its program managers are contractually required to comply. These requirements should include the issuer's expectations for the program manager's AML policy, four pillars and specific requirements for CIP, transaction monitoring, reporting, and OFAC. Depending on the program manager's other business lines, program manager's may or may not be required to have their own AML policy to address applicable AML regulations. In those cases, the sale of prepaid cards and the issuer's requirements should be added to program manager's existing AML policy.

### AML officer

Each program manager should have a designated AML officer. Depending on the size of the company, the officer may hold multiple positions, including but not limited to legal, fraud, risk, finance or operations. In all cases, the program manager's AML officer should have the resources needed to fulfill their responsibilities; however, the AML officer may have limited AML experience depending on the program manager's other business lines. In those cases, it is beneficial if the issuer can provide additional training. Offering the program manager industry training solutions, such as those provided by the Network Branded Prepaid Card Association (NBPCA)<sup>2</sup> or ACAMS, can be beneficial for everyone.

### AML training and retail agents

Program managers should be required to attend initial and annual training on the issuer's AML requirements. The program manager should also be required to provide AML training to their applicable staff and any retail agents. If the program manager is using retail agents to sell or reload prepaid cards, it is crucial for the issuer

Each program manager should have a designated AML officer

to ensure that the retail agent is provided with AML training for sale of its products. How to deliver this training should be a risk-based decision; however, it is recommended the issuer provide direct training to the retail agent when possible, versus using a train the trainer method whereby the program manager delivers the training. The issuer should also have a contractual agreement with each retail agent selling its prepaid cards.

### Independent testing

The issuer should ensure their annual independent audit includes testing of their prepaid card programs and controls. The issuer should also consider applying risk-based requirements for independent testing of its program managers. Independent testing is crucial for the issuer to show their regulator that they are providing appropriate oversight of the program manager, and it can also be used as a performance measurement for the issuer to evaluate the program manager's compliance. In the case of higher-risk program managers, the issuer may require the program manager to obtain an external independent review of their AML program and its adherence to the issuer's requirements. In lower-risk cases, the issuer may opt to do its own review of the program manager's AML program; however the adequacy of this review may be questioned due to the issuer's involvement in setting the standards. One way to solve this is for the

issuer to maintain separate areas or departments, one to develop and train on the AML requirements and one to perform independent testing for compliance.

### Customer Identification Program

One of the most important AML considerations for an issuer is determining how best to apply its Customer Identification Program (CIP). As a regulated financial institution, the issuer's CIP requirements for prepaid cards should be similar to its CIP requirements for traditional deposit products. In most cases, however, CIP on prepaid cardholders is performed in a non-face-to-face environment due to the online nature of the product or data security constraints at retail. Since many program managers will be using non-documentary verification methods such as public database checks, the issuer should consider selecting and approving a few vendors that meet its CIP criteria and work with those vendors to develop a compliant CIP decision model for the program managers to utilize. If the issuer is not involved in approving the verification method, its CIP testing will need to be increased to ensure that program manager compliance. The issuer should also provide the program manager with its requirements for documentary verification, e.g., what documents are acceptable under its CIP. In the case of payroll card programs, the program manager may also request approval to allow the employer to perform CIP verification. The issuer needs to set and provide standards for any third party reliance as well. However the issuer decides to handle CIP, it is crucial to establish a testing process to evaluate the program manager's compliance with the issuer's CIP. Issuers should consider continued exceptions and failure to comply with CIP requirements as a reason for contract termination.

### Currency transaction monitoring and reporting

Cash deposits, or "value-loads," are rarely accepted by either the issuer or the program manager. If cash value loads are accepted, it is usually through a third party "load network," which carries the appropriate money transmission licensing, as well as the

<sup>2</sup>The NBPCA is a trade association open to all companies involved in providing prepaid cards that carry a brand network logo and offers educational resources to both members and non-members. [www.nbpca.org](http://www.nbpca.org).



responsibility to aggregate and report cash transactions. In addition, prepaid card attributes are prohibitive of reportable transactions, as most value loads and withdrawals are limited at \$2,500 per transaction. However, issuers still need to consider the ability to aggregate cash activity between multiple cardholders. Does the issuer obtain the transactional records? If so, how can the issuer aggregate activity if one cardholder has a card with program manager A and another card with program manager B? These aggregation issues remain a challenge for the prepaid card industry.

### Suspicious activity monitoring, reporting and law enforcement needs

Suspicious activity monitoring can be handled one of two ways, depending on the amount of data the issuer receives on its cardholders. If the issuer receives all cardholder information including transactional data, typically referred to as “flat files,” it can monitor activity within its organization. The issuer may use a fraud or AML tool provided by a card association, an internally built system and risk-based rules, or an outside vendor solution. However, few vendor solutions currently available for AML monitoring adequately address the unique characteristics of prepaid card programs. It can also be difficult to justify the cost of a vendor solution when prepaid revenue can be pennies per transaction.

If the issuer is not receiving flat file information, or transactional data, it must provide its program managers with suspicious activity monitoring requirements. Issuers should consider monitoring for such things as multiple cards, cash value loads followed by cash withdrawals, merchant credits without corresponding debits, multiple transfers to and from accounts, deposits in names other than the cardholder and above average value loads. The issuer should also periodically test the program manager’s compliance with the monitoring requirements.

As the regulated financial institution, the issuer also has the responsibility to file SARs on reportable activity. The issuer’s AML requirements should provide the program managers with information such as when

and how to report suspicious activity to the issuer. Issuers should consider whether to have the program manager report all suspicious activity, regardless of the dollar amount, or to report suspicious activity only when it meets the reporting threshold. For instance, if the program manager is only required to report suspicious activity at the reporting threshold, the issuer is unlikely to be aware of suspects with multiple cards conducting suspicious activity that would be reportable when aggregated.

The issuer should complete the SAR with enough detail for law enforcement to understand what transpired. Some law enforcement personnel may have limited experience with prepaid cards, thus it is important to use understandable terminology and explain unique schemes. For instance, the prepaid industry typically uses the term “value load,” which is in effect, a deposit. It is also important for law enforcement to know the source of funds; if a card was loaded by payroll the issuer should provide the name of the employer. Likewise, if a card was loaded by cash, the issuer should provide the loading merchant and location if able. The issuer should also have a process in place to respond to law enforcement requests, both through 314(a), subpoenas and National Security Letters. Very little has been published on actual cases involving prepaid cards; however, one


good source is the FATF report published October 2010 entitled *Money Laundering Using New Payment Methods*.

### OFAC

While technically separate from AML regulations, the issuer should also ensure its program managers are maintaining compliance with OFAC requirements. It is recommended that issuers conduct their own periodic OFAC screening to fulfill their obligations; however, the issuer may not be able to perform the initial OFAC screening prior to the account being opened. In those cases the issuer must rely on its program manager to conduct the initial OFAC screen. The issuer should provide the program manager with requirements on the timing of the check, as well as directions on how to clear a hit and report a match. The issuer should include testing of the program manager’s OFAC process as part of its standard CIP testing. Lastly, while the card associations require blocking of certain OFAC sanctioned countries, it is also a good idea for the issuer to provide its own list of prohibited countries to the program manager.

### Conclusion

Hopefully this brief article provides you with valuable information regarding the AML and risk challenges faced by financial institutions issuing prepaid card programs. While the challenges can be significant, prepaid cards remain a viable product line for financial institutions and a necessary financial product for a significant segment of consumers.

Part two of this article will address AML and risk considerations for companies selling and marketing prepaid products, including some of the AML challenges raised by FinCEN’s Notice of Proposed Rulemaking on *Amendment to the Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Prepaid Access* released June 28, 2010. 

Jani Gode, CAMS, senior AML consultant, SightSpan, Inc. Mooresville, North Carolina, USA, [jgode@sightspan.com](mailto:jgode@sightspan.com)

The issuer should complete the SAR with enough detail for law enforcement to understand what transpired

# Homegrown risk: The growing threat of insider fraud

**Bank CEO Given Suspended 8 Month Prison Sentence and Banned from Banking Industry for Fraud**

(Dealbook.NYTimes.com, January 18, 2011)

**Former Banker Jailed for £54m Fraud**

(Bobsquide.com, January 14, 2011)

**Long Island Securities Dealer Charged in Fraud**

(LIBN.com, December 21, 2010)

**Former Rhode Island Senator Pleads Guilty to Bank Fraud**

(Ethisphere GRC Digest, November 10, 2010)

**Former Bank Computer Programmer Found Guilty in Code Theft**

(WSJ.com, December 11, 2010)

**T**hese are just a handful of cases ripped from recent headlines. Unemployment, debt and the economic downturn can influence individuals to resort to crime. A flourishing underground economy and highly sophisticated schemes are changing the face of internal fraud.

## Organizational vs. individual relationships

While most institutions are focused on external threats, they have become increasingly vulnerable to malicious insiders: current or former employees, contractors, trusted third parties or other business partners who have authorized access to an organization's network, systems, data or other assets. Celent, a search and advisory firm serving the financial community, estimates that approximately 60 percent of bank fraud cases involving a data breach or theft of funds are the work of an insider. In addition to fraud, sabotage and theft of intellectual property also present serious insider threats.



Perpetrators of insider fraud have been categorized in studies as having organizational or individual relationships. Typically, insiders with organizational relationships hold non-technical positions but have authorized access to systems for their jobs. They are after financial gain and will usually commit the crime while at the work location.

Insiders with technical or technical-related positions have individual relationships. Consultants, contractors and trusted third parties are included in this category because they can use their technical knowledge to cause damage to the institution. Insiders with individual relationships typically commit sabotage or steal intellectual property (client databases, proprietary software code, etc.). Cases of sabotage usually point to technically proficient former employees who use unauthorized, remote access outside of normal working hours while IP theft usually takes place during normal working hours by current employees with authorized access. Institutions with more effective awareness programs support a broader view of Know Your Employee (KYE). These institutions have greater insight into crimes committed by those with organizational versus individual relationships.

## Alarming statistics

In its “2010 Report To The Nations On Occupational Fraud And Abuse,” the Association of Certified Fraud Examiners (ACFE) compiled data from approximately 2,000 worldwide fraud cases that occurred between January 2008 and December 2009. The study revealed that the most commonly victimized sectors were banking/financial services, manufacturing and government/public administration. Based on information provided by the certified fraud examiners who investigated these cases, the report presented some interesting statistics:

- Organizations lost an estimated 5 percent of annual revenue to fraud. When applied to 2009 Gross World Product, this translates to \$2.9 trillion in potential fraud losses.
- Nearly one quarter of the frauds involved losses of at least \$1 million.
- The median time for detection was 18 months.
- 90 percent of the cases analyzed were asset misappropriation schemes.
- More than 80 percent of the fraud cases were committed by individuals who worked in accounting, operations, sales,

Institutions that understand the true scope and profile of internal fraud risk will be better positioned to protect all their assets

executive/upper management, customer service or purchasing.

Recognizing the growing threat of fraud, the U.S. Department of Justice FY 2010 Budget Request included an increase of \$62.6 million and 379 additional positions to fight mortgage fraud, corporate fraud and other economic crimes more aggressively.

## Analyzing the risk of insider fraud

Globalization has contributed to the complexity of analyzing insider threats. When assessing employee and third-party risk, institutions should consider the following factors:

- Collusion — insiders may be recruited by or working for outsiders such as crime rings or foreign organizations and governments.
- Business partners — the level of difficulty monitoring and controlling access to information and systems increases with “trusted” business partners.
- Mergers and acquisitions — there is a heightened risk when organizations merge into an acquiring organization.
- Cultural differences — it is more difficult to recognize behavioral indicators in a multicultural environment.
- Foreign allegiances — organizations operating outside their country of domicile may have overseas employees with other allegiances.

In addition, organizational culture, subtle interactions, psychological issues and company policies and business practices should be considered in the analysis. Institutions that understand the true scope and profile of internal fraud risk will be better positioned to protect all their assets.

## Implementing an aggressive defense

While industry experts agree that education is the best defense, enterprise-wide awareness is only half the battle. Institutions are advised that a holistic approach is the only effective way to detect and prevent insider

fraud. Recommendations for a holistic strategy take a four-pronged approach:

**Organization** — establish a pro-active anti-fraud culture.

- Begin with the hiring process; new employee screening and training
- Implement effective awareness programs with periodic re-training of employees
- Monitor and respond to suspicious or disruptive behavior
- Anticipate and manage negative workplace issues

**Policies and Practices** — clearly document and consistently enforce policies and controls.

- Evaluate threat of insiders, business partners and trusted third parties in enterprise-wide risk assessments
- Develop an insider incident response plan which includes a confidential, safe “whistle blower” process
- Escalate suspicious activity responses
- Implement strict password and account management policies on a need-to-know basis

**Technology** — create unified tracking and monitoring of environments and data.

- Consider insider threats in the software development life cycle
- Employ authentication and intrusion technologies
- Exercise extra caution with administrators and privileged users
- Implement strict system change controls

**Customers** — establish ongoing fraud prevention education.

- Seminars
- Privacy policies
- Statement inserts
- Web site message boards

The threat of criminal activity continues to increase with more complex fraud schemes on the rise. The FBI’s Criminal Investigative Division reported to the U.S. Senate Judiciary Committee that new corporate fraud cases increased by 111 percent in 2010. Insider fraud remains one of the weakest points, and, therefore, the greatest area of exposure for many institutions. It is definitely time to take note and revisit 2011 plans and budgets to ensure insider fraud detection gets the attention it deserves. **▲**

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

# Inside the white-collar criminal mind

(Predictive forecasting or palm reading)

While doing my research for this article, I ended up going to a psychic. I wanted to see how well they could predict my personality. It seemed the accuracy of predictions had an unusual correlation to the amount of cash that I paid. I should have known better, while doing a card reading he kept asking me, “hit or stand pat?” The bottom line of course is there are no mystical or magical methods of predictive forecasting. However, history is a great teacher. Analyzing real white-collar criminals can provide potential leads, clues and indications of events to come.

At most institutions, we monitor the front door and are suspicious of strangers (magnetometer, x-rays, pat-downs) and we monitor the backdoor for incursions (hackers, viruses, phishers); however, the invited guests, better known as the employees, rarely get a second look after the initial hiring phase. Especially, the higher up the rank structure a person is the less likely that they will be scrutinized. This can contribute to what is sometimes called the deviance of the elite. While the organization does not turn good people into bad, they can unwittingly underwrite the culture that allows white-collar criminals to justify in their minds the deviant behavior that they perpetrate, and then so skillfully evade any guilty feelings about their actions.

The idea of attempting to understand the mind of the white-collar criminal is not about the ability to create a red flag template checklist of personal habits of employees. The concept is to encourage you to think about the possibilities of the types of risk associated with any criminal element within

your institution and about the opportunity that you may have unwittingly created that allowed this to take place.

Part of what makes it difficult to develop a risk assessment or predictive forecasting for white-collar crimes is mired right in the general foundation of its existence. Even researching the subject becomes cloudy because there is no single crime called,

white collar. By nature, it encompasses many different types of crimes and various types of perpetrators. We probably all agree that the Bernie Madoff type certainly fits the bill. But what about the local guy who kites a few checks? Would he be classified as a white-collar criminal? What about the guy running a lottery scam out of his basement?

It would be helpful to have some sort of working definition of what is meant by the term, white-collar crime (at least for the objectives of financial institutions). The following is a definition provided by the National White-Collar Crime Center:

*Planned illegal or unethical acts of deception committed by an individual or organization, usually during the course of legitimate occupational activity by persons of high or respectable social status for personal or organizational gain that violates fiduciary responsibility or public trust.*

Following the above definition, and for the purposes of this article, we will consider white-collar crimes to be some type of occupational and/or organizational crime.

What is the difference between occupational crime and organizational crime? A generally recognized definition is that occupational crime is committed for the benefit of an individual and organizational crime is one that is committed for the benefit of the employing organization.

Further making it more difficult to truly get a quantitative handle on this issue for any type of data compilation, is the fact that many times a white-collar crime may be detected and not reported. Institutions may choose

What is the difference between occupational crime and organizational crime? A generally recognized definition is that occupational crime is committed for the benefit of an individual and organizational crime is one that is committed for the benefit of the employing organization





not to report an event because of the concern to their reputation and the damage that might occur. No one wants to see the name of their institution on the front pages of *The New York Times* for embarrassing indiscretions. To compound that matter, an employee that might be exposed by the institution is released (without police intervention) only to resurface at the institution across the street ready to resume the same criminal behavior.

Now that we have established a semi-solid framework for what a white-collar crime is, let us discuss the concept of predictive forecasting.

“He’s lying when he looks down and to the left,” or “He’s got sweaty palms in a cool office,” or “Watch him fidget, he must be nervous about his guilt.” I am sure you have all heard statements like that, especially if you watch some of those ridiculous

police shows on TV. Those scenarios are all individual building blocks in reading body language and no one or two items is proof of anything. Furthermore, if you are at the point that you are actually interviewing a subject and trying to read his body language, then you probably have already encountered a loss and are merely in reactive mode. The concept here is to try to recognize a certain profile as a possible problematic situation prior to having to circle the wagons and clean up the mess.

Due diligence, particularly at the onset of any employment relationship is essential and can save your company a lot of grief if you have a solid “know your employee” policy. That being said, unfortunately, it may not do much for you in the area of white-collar crimes, as historically, the wrongdoers will not have a criminal record. This could be for several reasons such as, the subject was never prosecuted, the subject was never caught or previous institutions swept it under the rug. Pick one, but the bottom line is, it is your problem now.

Let us discuss the atmosphere for a white-collar crime to occur. Usually there are three factors.

1. A generous supply of inspired and potential wrongdoers
2. A target rich environment
3. The lack of oversight or ineffective control systems and/or policies

Focusing on the last category, which is the only one that you have very much control over, it might be time for an honest review and analysis of your own systems. As far as the potential for an employee to turn to the dark side, it should be an institution’s responsibility to understand situations and outside influences that might contribute or push an employee in the direction of committing a crime. I will refer to this as “Continue to Know Your Employee.”

Certainly there are differences between wrongdoers with low self-control who respond to an opportunistic event, people who commit a crime to satisfy their own ego and those who do it depending upon their personal state of affairs. Examples of outside influences: Spouse laid off, kids’ college tuition, gambling, drug and/or alcohol issues, divorce and health concerns.

With the bad economy and 401K’s becoming 201K’s, bonuses out the window, cutbacks in overtime and generally asking employees to do more for less, that could certainly

contribute to or trigger an unscrupulous event. Lastly, corporate culture plays an important role. If the management chain of command shows a propensity to be weak, lazy or even border line unethical, then certainly the door is being opened and is seducing an employee who might be contemplating criminal activity.

In a culture that is so bottom line results driven, it becomes easy to overlook the long term. How does management get to observe any potential personality changes or even become aware of an employee's personal situation if there is little communication between them? There is no possible way to try to forecast a white-collar event if you have no clue who is your employee. This does not mean that management needs to take everybody out for a beer after the shift, but it should spark management to take a more proactive part in the ongoing concept of "know your employee." Very few incidents can ruin the reputation a financial institution faster than a bad employee. Operational risk leads to reputational risk.

Moving past the atmosphere, let us get to the crux of this and discuss some of the motivational factors and ideologies of a white-collar criminal mind. Keep in mind that many of the following qualities are interrelated and a person may exhibit several and/or bits of them all.

- **Greed:** This is quite subjective. One person's greed is not the same as another's. Do I really need five Ferrari's? However, the subject is motivated to obtain more and more objects of affection, regardless of the need or even the ultimate usage of the object. The desire for wealth is a ravenous appetite.
- **Need:** Unlike greed, a subject may be at such a low point that he/she feels that the only way out is to steal. Gambling, alcohol or drugs may be underlying causes; however, once that door is opened, the slippery slope begins. The more that the subject does not get caught, the easier it becomes to continue committing crimes, even long after the subject has crawled out of the original hole. In another variation of need, the subject may be unable to admit the failures at the workplace and turns to crime to disguise those inadequacies.
- **Imitation:** The subject becomes aware of other people doing bad deeds, so he/she


wants to show that he/she can do it too. The semi-glorification of wrongdoers by various media outlets does not help. The hiring of a black hat type prior criminal to review your systems may seem to have some merit; however, it may have an inspirational effect on the subject.

- **Resentment:** A subject may have determined that he/she is worth more than he/she gets paid, or feels that he/she has been treated poorly or disrespected in some way, shape or form. He/she then feels that he/she is only taking what he/she deserves.
- **Opportunistic:** Sometimes if the stars align just right, the self-discipline is low and the opportunity reveals itself, the subject will take the risk. He/she may fall in love with his/her own particular financial strategy and become obsessed with it and determined to prove that it works. When it does not, opportunity turns to need.
- **Gratification:** Money is not the motivating factor. The act, in and of itself is what motivates this subject. The game is the most important thing.
- **Validation:** The subject excuses his/her own actions and believes that he/she has done no wrong. He/she has no apology for his/her actions and anyone that was hurt due to his/her actions were wrong for getting in his/her way. He/she feels little to no guilt. He/she may dehumanize any event and believe that no real person was hurt.
- **Superiority:** He/she feels that he/she is the smartest person in the room (and he/she is very intelligent) and he/she is entitled to anything that he/she can obtain. The subject feels that he/she is above the law, and certainly above any rules and regulations. He/she believes that he/she has a higher purpose and ethics need not apply. He/she has the knowledge of how the system works and can manage to fly under the radar.
- **Ego:** An offshoot of superiority, the subject seeks ego gratification by outsmarting his/her bosses, the system and even the authorities. However, at the core of his/her being is a sense of inferiority that must be nurtured by external successes.
- **Power Dominance:** The subject loves the control and the admiration that goes with it. The subject circulates in powerful

circles and easily mingles with other power brokers.

- **Addiction:** The subject seeks out risk and the adrenalin that goes with it. Each day the system is overcome, new crises to conquer are needed.
- **Responsibility:** When things go wrong, it is not the subject's fault. Clients may be blamed for their ignorance, or blame shifted to other employees, organizations or on the government for too much or too little regulation.
- **Critical Mass:** The subject, when confronted and/or cornered, will attempt to redirect interest away from the real issue and focus instead on a different topic or even on the confronter. This allows the subject to maintain a guilt-free perspective.

In summary, there is no sure fire method to determine if a person is or about to become a white-collar criminal. However, those criminals who have been captured do tend to exhibit similar behavior patterns. Much like using good interviewing techniques and reading body language, there is no single character descriptor that is the panacea for discovery. Reading various profile characterizations is simply building blocks that when added together creates nothing more than potential warning buoys.

The lesson here is for management, upper level management, boards of directors, the financial gods or some white-collar crime fighting superhero to adopt a proactive approach to white-collar crime. Written policies and procedures should be created, developed and implemented, and this risk should be managed as you would any other type of risk. Institutions should advance concepts such as team building, and critical thinking. How do you adapt to change? Reflect upon your own trust behaviors. Develop strategies for creating leaders and not just managers. The more you can do to know your employee, create an air of cohesiveness, mutual respect and lawfulness, then you should reduce your chances of unwittingly forming opportunistic incidents. 

*Kevin Sullivan, CAMS, director of the AML Training Academy, Ret. Inv. New York State Police, NY HIFCA El Dorado Task Force, New York, NY, USA, Kevin@AMLtrainer.com*



**Save €150!**

Register by  
April 5  
with VIP code  
EUAD-150

5-7 June 2011 ■ Amsterdam, The Netherlands

7th Annual ACAMS  
**Anti-Money Laundering  
& Counter-Terrorism  
Financing Conference  
Europe**

***Mark Your Calendars***

Let the world's leading AML/CTF experts show you how to exceed regulatory expectations and strengthen your compliance programme.

**Register today for the most comprehensive training available featuring:**

- Interactive sessions covering topical issues with a focus on international best practices
- Insight into new requirements and legislation affecting financial institutions across the region
- Latest financial crime schemes and the tools to combat them

PLATINUM SPONSOR

**DOWJONES**



# Organized crime at your doorstep

Lessons learned from prosecuting organized fraud rings



No matter how different their size, geographical location, background or area of expertise, criminal organizations that target financial institutions take advantage of gaps in employee training and communication and the pressures that bank employees face. Despite their usual lack of sophisticated knowledge of the Bank Secrecy Act (BSA) and the attendant anti-money laundering/Know Your Customer (AML/KYC) issues confronting financial institutions, criminals rely on their understanding of human nature and how best to exploit it.

Four areas where institutions should be especially wary are: the on-boarding process, responding to reports of branch transactions, compromising of employees, and interacting with the call center. Fact patterns and interviews from several long-term investigations and prosecutions of these groups illustrate the problems and provide solutions to make your institution a less likely target.

### On-boarding: Mixed messages at the branch

Branch personnel are under constant pressure to open new accounts. Employees can be rewarded and penalized depending on their success or failure at this endeavor. While under this enormous pressure, branch personnel are also required to attend training in AML/KYC policies and procedures, including those related to the on-boarding process. The pressure and incentive to open accounts does not always reconcile well with the AML/KYC policies and procedures. Criminal fraud rings take advantage of this conflict by convincing honest employees — or aiding dishonest ones — to open accounts for them in violation of bank policy.

Examples of how criminals fraudulently open accounts include:

1. A bank where personal bankers were permitted to leave the branch without supervision and venture into ethnic communities to sign up new accounts. The bankers were responsible for examining all identification documents and verifying information.
2. A branch manager who allowed an account holder at the bank to bring in the identity documents of other people in order to open accounts for them.
3. Personal and business accounts opened for the same person using different names. Account holders claimed that they were known by other names in the international community.
4. Accounts opened in the names of different and unrelated people, who nonetheless share the same phone number, employer or address.
5. Business accounts opened where the business addresses do not exist or are post office boxes.

In each example, numerous accounts were opened. Shortly after being opened, the accounts were used to commit credit card fraud, business and personal loan fraud and money laundering. Because of the number of accounts opened, the criminal ring was able to move less money through each account and attract less unwanted attention. By the time the AML systems flagged the accounts and the banks moved to close them, the fraud ring had stolen several million dollars in unpaid credit card charges and loans from each institution.

Many industry officials have stated that, as there is no risk of loss to the bank during the on-boarding process, the transaction is not inherently risky. As seen above, however, once a criminal organization has infiltrated an institution, their capacity for fraud is great. Moreover, this fraud will likely extend far beyond the bank where the account is domiciled because the next institution will rely on the fact that the criminal has an account at one bank in deciding whether to allow him to open an account, or get a loan at their own. One bank's KYC failure can, therefore, adversely affect others.

### Communication gap: AML departments and the front line

Branch tellers and their supervisors are the first to know when an account holder has requested something unusual or provided an explanation that does not make any sense.

They are familiar with trends in their area and they interact daily with potential criminals, honest account holders and each other. Once they sense something is amiss, the branch generates an alert report. In most cases, however, that report is not sent to investigations but to the AML and/or compliance department to determine whether any action, including the filing of a SAR, should be taken. Criminals take advantage of this by completing their frauds as quickly as possible.

For example, one fraud ring specialized in obtaining Home Equity Line of Credit (HELOC) loans from different institutions on the same residential property through the use of fraudulent identification and without permission from the homeowner. Each loan was approved for several hundred thousand dollars. As soon as the loans closed, the target began visiting a local branch, almost every day, to cash checks drawn on the HELOC account. The amount of each check was consistently less than \$10,000. Branch personnel found that this behavior was unusual for the area and the type of account. They pressed the target for an explanation, and found that he gave different and insufficient answers. The tellers informed their supervisor and sent an alert report regarding the activity. After the target made numerous visits to the branch, the manager spoke to him about the size and frequency of the withdrawals. The target responded by increasing his withdrawal amounts to \$20,000 to \$30,000 per visit. Again, branch personnel followed bank policy and sent alerts about the behavior.

By the time someone from investigations got the case and spoke to branch personnel about their alerts, the accounts were entirely depleted. Moreover, because the target was using fraudulent identity documents, there was no way to identify him. Bank officials stated that they did not respond sooner to the alerts because the HELOC loan is not an inherently risky transaction, as it is the homeowner's own money, secured by real property. They relied on risk assessment to the exclusion of employee alerts. The fraud ring stole more than \$1.4 million.

## Know Your Employees — A matter of trust

Prospective employees are screened in a variety of ways during the application process. Once employed, methods are used to monitor productivity and trace misappropriated funds or allegations of fraud. But there is a lack of real-time review of either new or established employees to determine if they are engaging in inappropriate behavior before that behavior shows up as a loss for the bank. This provides criminal fraud rings with the ability to infiltrate an institution by placing a new employee of their own or compromising an existing one.

For example, a fraud ring pays young individuals to apply for teller positions in order to steal customer information. After limited training, these new employees often have the ability to access almost all accounts across the portfolio, including signature cards, with no numerical, geographical or other restrictions. No alerts are generated even if a new employee accesses hundreds of accounts with no transactions following any of them. These new employees will often work for only a few weeks and will leave the bank's employ before the criminal ring begins to make unauthorized withdrawals from the accessed customer accounts.

On the opposite end of the spectrum are long-term employees — often ones who have been internally promoted. They are in positions of trust and their performance reviews tend to highlight their productivity and not focus on whether the accounts they opened, or loans they closed, have resulted in fraud. The expectation that they will continue to produce, or some external financial pressure, can make them susceptible to criminal fraud rings' efforts to compromise them.

For example, a long-term bank employee who was a branch manager developed a drug habit. To make extra money, he began training a group of criminals in the bank's procedures regarding opening business accounts and obtaining loans. He advised the fraud ring regarding the documents they needed and interceded on their behalf with the loan department to make sure their business loans closed, even though he knew that they did not have any legitimate business. For his effort, he received a percentage of each loan that closed. As a branch manager, his name did not appear on any paperwork. He gave the account opening and loan closing credit to other branch personnel. None of the loans, which totaled more than \$2 million,

Institutions that understand the true scope and profile of internal fraud risk will be better positioned to protect all their assets

were ever repaid, and the accounts were used to launder the ring's money.

Real-time review of both new and existing employees would have aided the bank in identifying the fraud and determining who was responsible. A comparison of employee access records and productivity changes across the branch, within a narrow geographic zone, or portfolio-wide, would help to identify anomalous behavior that could then result in further investigation.

## The call center — Help at any cost

Criminal rings need their accounts to stay open in order to further their goals. Yet their behavior often triggers AML alerts that automatically freeze their activity. This leads to contact between members of the criminal organization and the call center. But call center employees are neither trained in, nor rewarded for, identifying potential fraud. Even in the most extreme cases, where callers cannot answer any security questions correctly, there is no procedure for alerting AML, compliance, or investigations to the suspect accounts.

Criminal fraud rings take advantage of human nature and the desire for the call-center employee to help them in order continue their fraud. Some examples include:


1. A caller who stated that he did not have his account number or date of birth with him, yet still managed to have the hold removed from his credit card;
2. Members of the fraud ring who advised each other to stay on the line with the call center and keep apologizing "until you get a nice lady who will feel sorry for you;"
3. A caller who could not state his address or phone number, even after receiving hints from the call center representative, yet still had his credit cards unfrozen;
4. Callers who stayed on the phone for more than an hour and were transferred to several different representatives before having their cards reactivated without having answered any question correctly;

5. A caller who refused to have the call center representative send someone to his business to check on his merchant machine but still got the account reinstated;
6. A caller who charged almost \$20,000 in cash advances on a new credit card without any explanation but who had the fraud alert lifted just by calling the call center.

Of course, once reinstated, these accounts were all used for credit card fraud and money laundering. No one at the call centers seemed to know what to do with a caller who could not answer a question, one whose identity was questionable, or one who acted irrationally. At the end of the calls, the representative simply reinstated or reactivated the accounts. Thus, the risk-based AML systems were effectively neutralized by the customer service-based call centers. If there was better training in identifying and routing potentially fraudulent callers, and a rewards-based system for call-center employees, these institutions would have been far more successful in preventing fraud.

## What can you do to better protect your institution?

Pay attention to the on-boarding process. If criminal fraud rings cannot get a foothold in your institution, they cannot defraud you as easily and they will go elsewhere. Real-time employee reviews can also cut down on the ability of your employees to aid the fraud ring. If new employees can be flagged — for accessing too many accounts relative to their co-workers, their geographic location, or their position — and long-term employees can be flagged — for a sudden change in productivity — the fraud rings can be stopped sooner. A review of loan and credit card default can also provide an institution with information regarding a possibly compromised employee.

Finally, the development of a hotline and reward system where branch and call-center personnel can quickly and easily alert investigations to something that is outside their normal customer experience and to possible fraud would provide a method by which an institution can not only stop a fraud in progress but may possibly identify the fraudster for law enforcement. 

*Meryl Lutsky, chief, Money Laundering Unit, New York State Attorney General's Office, New York, New York, USA meryl.lutsky@ag.ny.gov*



# Information **OVERLOAD**



ComplianceAdvantage.com  
is the **ANSWER**

Making it easy to manage  
what **YOU** need to know,  
when **YOU** need to know it.

- ELIMINATE the burden of regulatory compliance information overload
- REDUCE research time
- STAY ON TOP of the latest AML/CTF and compliance news

Attend a 20-minute online demo and receive a **FREE** trial subscription

Sign-up at [www.CAfree trial.com](http://www.CAfree trial.com).

# Human trafficking: AML's dilemma

A surprise topic made an appearance at the annual ACAMS conference in Las Vegas in September. And rumor has it the same topic was quite prominent at the ABA Conference in Washington, DC in October. Human trafficking, a seldom-referenced topic in anti-money laundering circles, has become a “hot button” topic. Human trafficking is probably the most surreptitious predicate offense to come along since the inception of suspicious activity reporting (SAR) requirements with billions of dollars generated annually from its various forms. With that kind of growth, any level of support that anti-money laundering (AML) professionals can provide law enforcement in identifying money laundering resulting from human trafficking is invaluable.

“After drug dealing, human trafficking is tied with the illegal arms trade as the second largest criminal industry in the world, and it is the fastest growing.”<sup>1</sup> Though human trafficking spans continents, defining the financial red-flag indicators of human trafficking is extremely challenging because it presents in multiple forms.

To develop human trafficking indicators, the illegal activity itself must be defined. First and foremost, human trafficking is not the same as smuggling. Those who are smuggled consent to their situations in one form or another, whereas trafficking involves use of force/coercion against the victim. Trafficking need not involve physical movement of a victim, whereas smuggling involves transnational or international movement.

The “Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children” is a protocol to the Convention against Transnational Organized Crime. Also called the Trafficking Protocol, it is one of the two “Palermo protocols” adopted by the United Nations in Palermo, Italy, in 2000. Signed by 116 countries, the Trafficking Protocol became effective in December 2003.<sup>2</sup>

According to the Trafficking protocol, trafficking in persons is defined as:

“(a)... the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs;

(b) The consent of a victim of trafficking in persons to the intended exploitation set forth in subparagraph (a) of this article shall be irrelevant where any of the means set forth in subparagraph (a) have been used;

(c) The recruitment, transportation, transfer, harbouring or receipt of a child for the purpose of exploitation shall be considered “trafficking in persons” even if this does not involve any of the means set forth in subparagraph (a) of this article;

(d) “Child” shall mean any person under eighteen years of age.”<sup>3</sup>

The Victims of Trafficking and Violence Protection Act of 2000 (TVPA) defines human trafficking by segregating the illegal activity into two subgroups: severe human trafficking and sex trafficking.

“(1) The term ‘severe forms of trafficking in persons’ means

(A) sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age; or (B) the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

(2)...The term “sex trafficking” means the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act.”<sup>4</sup>

From the definitions, only a minor under the age of 18 can be a victim of “severe trafficking” when trafficked for the purpose of commercial sex under the TVPA, whereas the Trafficking protocol does not make such a distinction. While the Trafficking protocol explicitly prohibits the trade of human organs when the donor is coerced and thus considers this human trafficking, the TVPA does not consider the trade of human organs as human trafficking. Another anomaly is illegal adoptions are not considered, by either definition, as human trafficking unless the illegal adoption amounts to involuntary servitude (e.g., slavery) because it lacks the use of force, fraud or coercion to compel services from the illegally adopted child.

Though the exact definition of human trafficking may not be consistent across acts, the definitions do agree on many of the underlying activities included in human trafficking. Kidnapping is human trafficking. Forced prostitution is human trafficking. Forced labor/servitude is human trafficking.

Research uncovered surprising and, quite honestly, disturbing images of human trafficking regardless of which definition is used. In addition, to the atrocious methods in which the trafficking is effected, the various methods used to control victims are equally as disturbing:

- *Physical*: beatings, burnings, rapes and starvation
- *Emotional*: isolation, psychological abuse, drug dependency and threats against family members in home countries
- *Financial*: debt bondage and threat of deportation.<sup>5</sup>

Having identified the underlying offenses to human trafficking, one might think identifying the transactional red flag indicators of the activity should be rather simple. Not so.

<sup>1</sup>[http://www.acf.hhs.gov/trafficking/campaign\\_kits/tool\\_kit\\_law/law\\_enforcement.ppt#287,3,Human Trafficking: What Is It?](http://www.acf.hhs.gov/trafficking/campaign_kits/tool_kit_law/law_enforcement.ppt#287,3,Human%20Trafficking:%20What%20Is%20It?)

<sup>2</sup><http://www.state.gov/documents/organization/142979.pdf>

<sup>3</sup>[http://www.uncjin.org/Documents/Conventions/dcatoc/final\\_documents\\_2/convention\\_%20traff\\_eng.pdf](http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_%20traff_eng.pdf)

<sup>4</sup><http://www.state.gov/documents/organization/10492.pdf>

<sup>5</sup>[http://www.fbi.gov/news/stories/2006/june/humantrafficking\\_061206](http://www.fbi.gov/news/stories/2006/june/humantrafficking_061206)





The characteristics of potential victims have been identified and are widely publicized on web sites dedicated to counter human trafficking. One list of victim red flag indicators can be found at <http://nhtrc.polarisproject.org/call-the-hotline/identifying-human-trafficking-.html#who>. Not surprisingly, research was unable to uncover a published list of transactional flags associated with human trafficking which could be developed into a suspicious activity indicator (SAI) for automated detection. What research did support is the assertion that local law enforcers, not AML investigators, are the most likely to uncover human trafficking.<sup>6</sup> So then, what is known about human trafficking that may aid in defining the financial transactions that might accompany the activity?

- Human trafficking has been identified in the following industries: domestic workers (nannies, maids), landscaping, nail salons, restaurants, industrial cleaning, construction, hospitality, magazine and flower sales, agricultural, factories (garments etc).<sup>7</sup>
- The victims are not paid for their services or are drastically underpaid for their services.
- Human traffickers are very often found to be associated with other crimes (e.g., prostitution, pornography, domestic abuse, battery and illegal businesses).
- Victims need not be “purchased” but may be kidnapped or traded by parents or another responsible party (e.g., pimp).
- Victims may be working to pay-off debts that are generations old.
- Last year, the world imported and exported billions of dollars in products tainted by forced labor in manufacturing and raw materials procurement, according to the International Labour Organization (ILO). Forced labor is also prevalent in cotton, chocolate, steel, rubber, tin, tungsten, sugarcane and seafood industries.

The last three bullet points make “following the money” in trafficking cases extremely difficult. Kidnapped victims are the source of future illicit funds which, if integrated into the banking system through routine bank deposits of a cash-intensive business, may never be traced back to the original trafficking offense.

Victims working to pay-off debts that are generations old, if working in a legitimate

business, would taint any profits arising from the business. Similar to the last bullet, identifying that trafficked victims are being used to generate raw materials or final products of legitimate companies is a daunting proposition for any AML program. In all respects, the funds flowing through the bank account of a legitimate company would look untainted. The business is operating as any business might.

One indicator, to which a bank AML investigator may not have clear line of sight, would be if payroll taxes and/or payroll do not match expenses expected for a company of similar operation. However, in an era where corporations bank with multiple financial institutions and multi-national corporations have mega-subidiaries, determining the appropriate payroll and/or payroll taxes for a production oriented company may not, and probably will not, be feasible.

Another red flag that something is amiss is when multiple employees provide the business address as their residential address. This may be an indicator the employees do not have a documented residence. For financial institutions, line of sight to customers’ employees’ residential addresses is not necessarily transparent and would be even more impeded for human trafficking victims as paper trails leading to victims, such as checks and paychecks, are avoided to ensure the activity stays under the radar. Typically,

traffickers will not establish accounts in the victims’ names; therefore, customer identification program (CIP) steps and other account opening validations that might otherwise assist in identifying a negative trend, such as supplying a commercial address for a home address, are not applicable.

In fact, the FATF Money Laundering & Terrorist Financing Task Force Typologies Report for 2004–2005 confirms “No novel money laundering techniques have been identified which can be uniquely associated with these offences. Though the STR reporting system generates some inquiries, trafficking in human beings and illegal migration remains primarily a law enforcement issue.”<sup>8</sup>

Though there are no common red flags for every human trafficking case, a recent law enforcement case in the United States has identified the use of “funnel accounts”<sup>9</sup> to perpetuate the flow of money in a major trafficking ring (*see sidebar on page 30 for information on funnel accounts*).

Human traffickers have recently started to receive the widespread negative press that drug kingpins, Ponzi schemers and tax evaders have garnered in anti-money laundering circles. Very recent high profile arrests further fuel the fire of the American public’s disgust and call for action. The question remains, are anti-money laundering profes-

<sup>6</sup>[http://www.acf.hhs.gov/trafficking/campaign\\_kits/tool\\_kit\\_law/law\\_enforcement.ppt#272,19,Identifying Crime of Human Trafficking](http://www.acf.hhs.gov/trafficking/campaign_kits/tool_kit_law/law_enforcement.ppt#272,19,Identifying Crime of Human Trafficking)

<sup>7</sup><http://nhtrc.polarisproject.org/call-the-hotline/identifying-human-trafficking-.html#who>

<sup>8</sup>[http://www.acams.org/ACAMS/ACAMS/UploadedImages/pdf%20downloads/HT/FATF-GAFI\\_Document.pdf](http://www.acams.org/ACAMS/ACAMS/UploadedImages/pdf%20downloads/HT/FATF-GAFI_Document.pdf)

<sup>9</sup>Information provided by major financial institution



sionals the proper “first responders” to this firestorm? The answer: probably not.


John Byrne, executive vice president for ACAMS states “that human trafficking is a crime that resonates everywhere. Trafficking is going on all around us and begs for a response.” Byrne also stated that ACAMS is the perfect forum for open discussions with law enforcement about how anti-money laundering professionals can assist with detection of a crime that is not necessarily money-based. With more than 10,000 members, ACAMS will continue to provide helpful guidance and thoughtful responses to law enforcement as they lead the effort to eradicate this horrible crime. In addition, ACAMS launched a web site dedicated to fighting Human Trafficking and Human Smuggling in November 2010.<sup>10</sup>

Adding to the difficulty in finding and successfully prosecuting human trafficking cases is that many victims are hesitant to come forward. Given time, a victim may

actually perceive his/her traffickers or new “owner” as a savior, someone to be trusted and relied upon. The trafficker or owner provides for the victim’s basic needs (food, shelter, clothes). When the victim is a child, conflicting emotions such as attachment to the trafficker, fear of punishment and an inherent desire to trust adults may prevent reporting, even in those few instances when reporting is feasible. In some societies, trafficking is widely accepted and encouraged (think forced marriages), which essentially extinguishes any hope by the victim of rescue.

Education and support are definite roles anti-money laundering officers should assume as the human trafficking drama continues to unfold. As with any hot button topic, AML professionals should take this opportunity to validate their detection processes and training program to ensure information regarding human trafficking typologies is considered for appropriate integration into AML programs. Because it is unlikely a

specific automated detection scenario will be developed to ferret out activity indicative of human trafficking, integration may consist solely of educating staff on the underlying trafficking activities to foster a comprehensive understanding. Effective training which incorporates information on red flags such as payroll or taxes not matching staffing levels and the attributes of funnel accounts takes on added significance to investigators.

While human trafficking remains a human rights issue, AML professionals can certainly lend moral support to the cause by raising awareness and understanding that trafficking is the predicate offense to some of the SAR reportable activity seen on a daily basis. Financial institution investigators must continue to report suspicious or unusual activity to provide the necessary leads law enforcement will use to track down human traffickers. 

*Jean-Ann Murphy, CAMS, USA, send comments to editor@acams.org*

### Dirty secrets of human trafficking:

- Families sometimes calculate how much debt they can incur based on their tradable family members.<sup>11</sup>
- Millions of trafficking victims are working to pay off their ancestors’ debts.<sup>12</sup>
- 100,000 American children are forced into prostitution each year in the U.S.<sup>13</sup>
- Everyday products like cell phones, wedding rings, laptop computers and batteries are made with blood minerals from Eastern Congo where there is forced labor, debt bondage, children working in dangerous conditions, forced marriage and child sex.<sup>14</sup>
- The average citizen has probably inadvertently provided financial support to human traffickers. Hundreds of everyday products are produced with forced labor and/or child labor. View the list of 122 goods at: <http://www.dol.gov/ilab/programs/ocft/PDF/2009TVPR.pdf>

### Funnel accounts<sup>15</sup>

Funnel accounts is a relatively new term in anti-money laundering circles.<sup>16</sup> Though the use of funnel accounts was found in a major human trafficking case, investigators and anti-money laundering professionals cannot lose sight of the fact that human trafficking exists in so many forms that the identified facts of one case should not be interpreted to mean all trafficking cases will use the same type of financial vehicle. In addition, when funnel account activity is identified, investigators cannot assume human trafficking has been uncovered. While many of the factors below taken singularly may represent unusual/unexpected activity, when found in combination, the likelihood that the identified activity represents some form of illegal, and thus, reportable activity increases dramatically.

- Funnel accounts not only indicative of trafficking (e.g., also used in smuggling cases)
- accounts set up as personal or business accounts; could be savings or checking accounts
- accounts opened with less than \$500, then followed within days by large out-of-state cash deposits
- deposits consist almost exclusively of large even-dollar cash deposits (e.g., \$1800, \$2000) made in states other than Arizona
- deposits are made at venues outside of branch tellers (drive-up, ATMs) by unidentified depositors
- in the cases where depositors were identified, the depositors were usually not established bank customers, and Mexican addresses were often used
- deposits are disproportionate with stated employment — which is often “babysitter,” “landscaper” or “unknown”
- the activity occurs outside of the state where the account was opened
- there is no other/expected/normal activity in states where the deposits are made
- no routine activity in the account — such as payroll check deposits, rent, utility bill payments, or routine cash withdrawals
- all withdrawals occur at various branches in Arizona or immediately south of Arizona in Mexican border cities, often through multiple, large-dollar ATM withdrawals, teller cash withdrawals or bank checks
- accounts are usually open for less than one year or become dormant with almost no remaining balance

<sup>10</sup><http://www.acams.org/ACAMS/ACAMS/topics/humantrafficking/Default.aspx>

<sup>11</sup><http://www.state.gov/documents/organization/142979.pdf>

<sup>12</sup><http://www.state.gov/documents/organization/142979.pdf>

<sup>13</sup>[http://humantrafficking.change.org/blog/view/urgent\\_need\\_to\\_support\\_critical\\_services\\_for\\_americas\\_sex\\_trafficked\\_children](http://humantrafficking.change.org/blog/view/urgent_need_to_support_critical_services_for_americas_sex_trafficked_children)

<sup>14</sup>[http://humantrafficking.change.org/blog/view/sec\\_asks\\_america\\_whats\\_your\\_solution\\_for\\_conflict\\_minerals](http://humantrafficking.change.org/blog/view/sec_asks_america_whats_your_solution_for_conflict_minerals)

<sup>15</sup>Representatives from the Department of Homeland Security and the Federal Bureau of Investigation requested the following information on funnel accounts be appended to the Human Trafficking article

<sup>16</sup>Indicators of funnel account activity reviewed and validated by a major financial institution

# VALIDATE YOUR AML LAW ENFORCEMENT EXPERTISE WITH CAMS CERTIFICATION



“I would recommend ACAMS to anyone in law enforcement who investigates financial crime or narcotics cases. The success of this operation can be attributed to what we have learned from ACAMS. Each of my detectives uses the CAMS certification in their search warrant affidavits. This truly gives credibility to their knowledge of money laundering.”

*Sergeant James A. Cox, III,  
Fairfax County Police  
Department*

## CAMS BENEFITS:

- Establish yourself as a public sector AML authority when conducting expert witness work and handling subpoenas and search warrants
- Stay on top of emerging financial crime trends and learn new techniques for combating terrorist financing
- Build a network with other public sector colleagues from across the globe and help bridge the gap with the private sector.

**Association of Certified  
Anti-Money Laundering  
Specialists®**

**ACAMS®**

# The prepaid card — Growing in use and risk



In recent years, prepaid card products have emerged into the mainstream of the U.S. financial system at an increasing rate. FinCEN estimates there are more than 2.5 million new prepaid cards issued each year, and at any given moment there are an estimated 7.5 million network branded cards such as Visa or MasterCard in use.<sup>1</sup> Prepaid cards have experienced a growth rate of 35 percent since 2004, from \$64 billion in annual loads to more than \$178 billion based on information provided by MSN Money Tool.<sup>2</sup> The security and convenience of prepaid products appears to have been accepted and embraced by many consumers.

The popularity of the prepaid card has been sparked by a number of factors that are primarily linked to the efforts to provide cost-effective financial products to individuals who are either unbanked or underbanked. In addition, prepaid cards are used by employers, federal, state and local governments and other agencies as a payment method — the cards can be easily reloaded with values to accommodate a variety of payment needs. The accessibility and convenience of prepaid cards have made bank provided benefits available and possible for just about anyone, expanding the boundaries of financial banking opportunities.

Unfortunately prepaid cards are not immune to risks — many of the same factors that make prepaid access and use so attractive to consumers also make it vulnerable to illicit activities. The risks and vulnerabilities to financial institutions can be tied primarily to the anonymity within and relative ease of accessing funds and transacting with a prepaid card. This combination of risk factors creates the potential for a substantial volume of money moving through multiple

products — all with unknown “owners” or “beneficiaries.” In addition, the anonymity of prepaid cards offers an advantage to individuals with questionable intent, as they can conduct transactions with significant amounts of money while potentially avoiding some of the cash, purchase-with-cash and cash transport reporting and record keeping requirements to which a non-prepaid account might be subject.

Examples of these reports include Currency Transaction Reporting, Purchase or Sales of Monetary Instruments, Report of International Transportation of Currency or Monetary Instruments and other FinCEN reporting — each designed to collect customer information to assist law enforcement in tracking and eventually impeding criminal activity. These risks create an increased potential for the use of prepaid cards as a means for furthering money laundering, terrorist financing and other illicit transactions through the financial system.

Before introducing a prepaid card product, financial institutions should consider its risks and must be willing to build the necessary controls into their compliance program. Without adequate monitoring, an institution runs the risk of overlooking irregularities in both card usage and customer behavior that could be associated with various types of criminal activities such as identity theft, debit and/or credit card fraud, income tax avoidance or evasion, money laundering and others, including terrorist financing-related activities. Neglecting to appropriately identify these financial crimes could result in serious consequences, from monetary penalties as a result of regulatory violations to significant financial losses to the issuing financial institution. Financial institutions that are consid-

ering offering prepaid card products should consider the following FinCEN guidance:

- Create clearly established rules and regulations, such as sensible limitations on card functionality to mitigate the risks for fraud and money laundering.
- Establish a Customer Identification Program (CIP).
- Implement strong automated fraud monitoring and reporting systems that evaluate data points similar to those relevant to detect suspicious transactions and other information relevant to the BSA.<sup>3</sup>

## Establishing rules and regulations

Before applications are accepted or accounts are opened, the functionality and transactional limits for the prepaid cards must be determined by the financial institution. Setting these parameters can be a challenging task when balancing the desire to attract new customers while also attempting to mitigate the risk of the product being used for illegal activities. Satisfying customer's wants and needs while also ensuring that those needs do not create vulnerabilities for the financial institution can be difficult. Fortunately, multiple government sources and other issuing financial institutions have published information about developing a robust prepaid card program to guide other institutions.

One of FinCEN's recommendations is to subject all prepaid card products to limits that are clearly visible on the product. Examples of these limits include a load limit, a total maximum value limit and a cash withdrawal limit. FinCEN suggests these limits should not exceed \$1,000 — an amount chosen for a number of reasons including industry research findings for average and maximum initial loads and consistency with thresholds

<sup>1</sup>U.S. Department of Treasury, Financial Crimes Enforcement Network. (2010). Amendment to the bank secrecy act (31 CFR Part 103). Washington, DC: Retrieved from [http://www.fincen.gov/statutes\\_regs/frn/pdf/Prepaid%20Access%20NPRM.pdf](http://www.fincen.gov/statutes_regs/frn/pdf/Prepaid%20Access%20NPRM.pdf)

<sup>2</sup>BusinessWeek. The basics prepaid gift cards: terrorist tool. Retrieved from <http://moneycentral.msn.com/content/Banking/P137668.asp?Printer>

<sup>3</sup>U.S. Department of Treasury, Financial Crimes Enforcement Network. (2010). Amendment to the bank secrecy act (31 CFR Part 103). Washington, DC: Retrieved from [http://www.fincen.gov/statutes\\_regs/frn/pdf/Prepaid%20Access%20NPRM.pdf](http://www.fincen.gov/statutes_regs/frn/pdf/Prepaid%20Access%20NPRM.pdf)



established for other Money Services Business categories. The \$1,000 threshold has also been shown to yield the greatest utility of information for law enforcement and their financial crime investigations. Furthermore, \$1,000 appears to be a reasonable and sufficient amount to cover consumer's needs while also helping to maintain low product risks.<sup>3 (ibid)</sup>

It is important to note these limitations cannot be applied to everyone; therefore, some exceptions are necessary. When dealing with government agencies or other verifiable employers that issue direct deposits exceeding \$1,000, financial institutions will want to decide if additional parameters to suit those specific customers should be established.

### Establishing a Customer Identification Program (CIP)

A vital step in establishing a sound and secure prepaid card program is implementing a Customer Identification Program (CIP) that captures the required information and reasonably verifies the applicants, prior to the card being issued. By gathering sufficient identification details about a customer and implementing a rigorous system to verify those customer details, financial institutions can lessen the anonymity factor related to prepaid cards. The CIP must include obtaining the required pieces of information such as the customer's name, date of birth, physical address and government-issued identification number, while also making sure the steps taken to verify an applicant's identity are risk-based and reasonable. If a financial institution uses a software program to assist with their verification, the institution must ensure it is updated and comparable to industry standards. Controls and monitoring should be developed for routine authentication of the respective validation software programs to guarantee its efficacy.

A highly effective CIP is critical to the know-your-customer process and is an important factor in meeting the regulatory expectations of a prepaid card account origination program. In addition, during customer verification and on-boarding, the chances of initial detection and prevention of fraud and related crimes increase exponentially. Identifying fraud and other crimes at the customer on-boarding stage help manage the customer

anonymity risks, in turn creating a stronger overall prepaid card compliance program.

In addition to capturing and verifying the customer's information, the participating financial institution must have an adequate customer information retention process. Aside from FinCEN's retention requirements, maintaining a record of the customers' information can also enhance the current program by creating a precedent, or baseline for future questionable transactions. Furthermore, this information could also aid law enforcement in the investigation and prosecution of any criminal matters arising from the prepaid card account(s).

### Implementing monitoring and reporting systems

In addition to an effective CIP, supplemental steps must be taken to further mitigate fraud attempts pre- and post- account opening. These additional steps include implementing strong monitoring and reporting systems built to trigger and raise flags on anomalies in prepaid card usage. Monitoring accounts at the application stage is critical to detect and avoid various types of fraud and problematic activity. An example of a monitoring scenario at application stage includes Internet Protocol (IP) address monitoring for those products that allow online applications. While online application channels may create an increased volume of new accounts, this channel also generates greater opportunities for identity thieves, fraudsters and their illicit activities. Considering online application processes leave little room for face-to-face customer verification, a financial institution should consider leveraging tailored suspicious activity indicators (SAIs) such as triggers on multiple card applications from the same IP address.

Identifying same or common phone numbers and addresses through application data monitoring can also indicate that fraudsters are targeting the prepaid card product for their illicit activities. An example of this type of monitoring includes instances when an applicant (or several applicants) uses the same phone number and address information to open multiple accounts simultaneously. Applicants displaying this type of behavior might be attempting to exploit either the customer on-boarding processes, the card functionality or they could be using illegitimate funds to open these accounts.

Monitoring of prepaid card activity after account activation should resemble the methods used in identifying and detecting suspicious transactions on regular debit and credit cards. Adequate SAIs should be developed, and periodic screening of the portfolio leveraging these indicators should be conducted for efficient risk management of the cards. Examples of SAIs that could be implemented include: maximum cash load and cash withdrawal monitoring, transactions in high-risk geographies, aggregate loads in a specified period of time, and purchase monitoring. When considering the initial detection thresholds for SAIs, the card transactional limits must be considered. Oftentimes the individual or groups targeting these products will operate just below the maximum allowable limits in an effort to avoid detection. Depending on the financial institution's needs and vulnerabilities, the aforementioned periodic scanning could be segmented into daily, weekly or monthly screenings.

### Making the trade-offs

As mentioned above, prepaid card growth shows no sign of slowing down and it appears prepaid cards have found a place within the financial system. Financial institutions researching the feasibility of starting a prepaid card program have many things to consider as they prepare to lay the foundation for their program. While the potential profitability of prepaid cards can make them attractive, the pitfalls can be significant and can negatively affect the financial institution. These pitfalls can be avoided by establishing an adequate and risk-based compliance control framework. Policies that include sensible card functionality and limits, an effective CIP, pre-activation account screening, and post-activation account monitoring can help lessen the potential risks associated with this product, and can lead to a safe, secure and prosperous prepaid card program. **FA**

*Kevin Nash CAMS, CFE, CIPP, sr. manager, AML Investigations, Capital One Financial, Richmond, VA, USA, kevin.nash@capitalone.com*

*Dorina Vornicescu, AML investigator, Capital One Financial, Richmond, Virginia, USA, dorina.vornicescu@capitalone.com*



**Tackling the AML compliance challenges of emerging payment alternatives:**

# Follow the yellow (gold) brick road into digital currencies

PART I

Enterprising entrepreneurs armed with rapidly evolving technologies are forever changing how we conduct our financial transactions. They also are contributing to countless sleepless nights of a growing number of anti-money laundering (AML) compliance personnel.

Whether purchasing goods, paying bills or transferring value from person-to-person using a prepaid card, a mobile phone or the Internet, new payments alternatives have been introduced at almost mind-numbing speeds over the last several years — both within and well beyond the borders of traditionally regulated financial institutions.

These payment innovations share a common theme: they respond to the unceasing demand for faster, safer and more cost-effective ways to transact business and transfer value. They also have no respect for time zones or geographical boundaries. And they are green!

At the same time, these innovations provide expanded opportunities for criminals — who are always looking for the latest and greatest payment mechanisms to facilitate their fraudulent schemes, money laundering, terrorist activities and other criminal ventures.

In turn, new payments alternatives challenge law enforcement and prosecutors who must (1) use precious time and resources to learn how these payments alternatives work in order to understand how and why criminals use them and (2) work with laws and regulations that inevitably lag behind the innovations and the criminals' use of such innovations.

And for the AML compliance professional, these new payments solutions may contribute to more than restless or sleepless nights; they may trigger nightmares.

Even if the business line gives advance notice of its intent to launch a new payment solution, the AML compliance professional inevitably plays catch-up to understand how it works, what its intended purpose is, who is expected to sign up for it and how it will actually be used, not to mention how customer use will be monitored. Learning about the solution after launch can be even more distressing — mentally and physically — as the solution inevitably involves nontraditional business partners and vendors, hard to understand payment flows and sometimes

yet to be determined money laundering and terrorist financing risks.

Possibly even more challenging for the compliance officer is monitoring customer accounts that show funds moving to and/or from a third party payment provider. In such cases, the AML compliance professional is likely to have little if any information about the ultimate source or destination of the funds.

*Enter Digital Currencies.* Digital currencies make up a class of innovative payments alternatives that were instantly destined to attract the attention of both criminals and law enforcement when they made their debut in the mid-1990s. Faster, more efficient, lower cost, instantly global and potentially anonymous, digital currency systems drew on the best of monetary theory and emerging technologies to monetize the intrinsic value of precious metals for use in an Internet-based economy.

Criminals are always looking for the latest and greatest payment mechanisms to facilitate their fraudulent schemes

During this period, AML compliance officers in traditional financial institutions (i.e., banks, securities firms, insurance companies) had little reason to pay much attention to these digital currencies because they were used essentially as closed systems with limited or no interaction with such institutions. However, as digital currency use is expanding and acceptable in a variety of financial transactions, the need for AML compliance professionals to better understand — and not lose any more sleep over — this payments alternative is becoming more pressing.

The first step toward getting more sleep is understanding what digital currencies are and the differences between digital curren-

cies and the group of rapidly proliferating “virtual currencies.”

*What are digital currencies?* The term “digital currency” is frequently used but is not often defined except in the context of other terms like “electronic money,” “e-currency” or “virtual currency.” The Financial Action Task Force (FATF) in its October 2010 report on “Money Laundering Using New Payments Methods” (FATF 2010 Report) provides a detailed analysis of how digital currencies work but does not offer a specific definition.<sup>1</sup>

Wikipedia defines the term “electronic money” to include “digital currencies” among seven other types of “electronic currencies.” A commonly used alternative term is “digital gold currencies,” or “DGCs,” which is a gold-backed digital currency.

A more precise term for describing “digital currency” is “private currency,” which is a medium of exchange issued by a person or entity other than a sovereign government. A digital currency may or may not be backed by a precious metal or similar store of value. It typically is not “sold” directly by the currency’s “issuer.” Instead a “currency exchanger” exchanges “fiat” (i.e., currency issued by a sovereign government) into digital currency, or vice versa, in the same manner as a traditional currency exchanger would exchange U.S. dollars for Euros.

Digital currencies can be used like any fiat — to pay for goods or services — if the person providing the good or service is willing to accept the digital currency as payment.

Although certain aspects of digital currency systems may differ, they share some common characteristics. A customer accesses the system’s webpage via the Internet and sets up an account. The account is then funded through a “spend” of the digital currency from another account that already holds the digital currency. A spend may occur when the digital currency is transferred from one account to another, either in connection with a purchase or sale of goods or services, a simple transfer from one person to another or a currency exchanger’s exchange of fiat for the digital currency.

The oldest, and probably best known, digital currency is e-gold. Digital currencies currently operating include GoldMoney, Pecunix and Liberty Reserve.

<sup>1</sup>Financial Action Task Force, Money Laundering Using New Payments Methods (2010), available at [http://www.fatf-gafi.org/document/2/0,3746,en\\_32250379\\_32237202\\_46705794\\_1\\_1\\_1\\_1,00.html](http://www.fatf-gafi.org/document/2/0,3746,en_32250379_32237202_46705794_1_1_1_1,00.html)



*How is a digital currency different from a virtual currency?* The term “digital currency” is sometimes used interchangeably with the term “virtual currency.” The two are distinguishable in part by how they developed and how they are used.

“Virtual currencies” are issued to play games in virtual worlds like Entropia and World of Warcraft. They often are referred to as “tokens.” They typically are purchased and redeemed from the owner of the virtual world or the operator of a site within the virtual world. Also, secondary markets have developed to permit players to buy and sell virtual currencies directly from each other.

Increasingly, virtual currencies are also being deployed in social/gaming networks and the scope of their usage is expanding. For example, Linden Labs, which owns and operates Second Life, sells Linden Dollars that can be used to purchase both virtual and real world goods and services. In this way, the line between digital and virtual currencies seems to be blurring.<sup>2</sup>

The incursion of virtual currencies into the real world was underscored in 2009 when the Chinese government, facing rapidly growing use of virtual currencies in the “real” world, issued a decree restricting the use of virtual currencies to the virtual world. Taking the opposite approach, the Korean government sanctioned the use of virtual currencies in both the virtual and the real worlds.

The proliferation of virtual currencies may be attributable to the ease with which one can be set up — at least 30 companies market technology platforms for deploying virtual currencies. While the platforms for virtual and digital currencies differ, virtual currencies are not immune to the types of criminal abuse that digital currencies have experienced.

*The AML compliance officer’s challenge?* Digital currencies present different types of AML compliance challenges for different types of entities.

Because digital currency systems operate as closed systems (i.e., the digital currency circulates only among account holders in the system), a digital currency servicer or provider is able to see all transactions in the system. The digital currency used in one transaction can be tracked through multiple transactions and multiple accounts over long periods of time. However, the digital currency provider,

will not necessarily know the original source of the fiat that was exchanged for the digital currency or who receives fiat upon exchange of the digital currency unless it acts as an exchanger or has built transparency into its system to allow it to view this information.

The digital currency exchanger is uniquely positioned to see who is exchanging fiat for digital currency and vice versa. The exchanger however will not have the ability to see the transactions between accounts within the system.

A traditional financial institution is unlikely to see any aspect of a digital currency transaction unless it is a digital currency provider or exchanger, accepts digital currency deposits, uses digital currency as a form of currency in their regular business activities or, possibly, provides banking services to digital currency provider. On the other hand, a traditional financial institution may see transactions between their customers and digital currency exchangers, although such transactions will be in fiat.

Regardless of who sees what, understanding the money laundering and terrorist financing risks presented by digital currencies and developing or enhancing an AML compliance program to mitigate such risks requires an understanding of how digital currencies work (including their transaction flows), how criminals have abused them, the unique challenges they present for law enforcement, how they are currently regulated, and what steps may be taken to mitigate money laundering and terrorist financing risks associated with their business models.

*Why is law enforcement concerned?* The 2005 U.S. Money Laundering Threat Assessment (Threat Assessment) analyzed 13 money laundering methods involving among other things “new and innovative online payment services,” including digital currencies.<sup>3</sup> Although not well documented and somewhat rambling, the report identified a number of specific vulnerabilities that could make such services subject to abuse for money laundering and other financial criminal purposes.

Appearing to draw heavily from the details of an investigation underway at the time involving e-gold Ltd, the “oldest and best known” digital currency services, the Threat Assessment outlined the following concerns:

The digital currency exchanger is uniquely positioned to see who is exchanging fiat for digital currency and vice versa

- *International Person to Person Payment Capability.* The ability to transfer value across jurisdictional lines creates difficulties for law enforcement authorities attempting to pursue enforcement or legal action outside their jurisdiction.
- *Lack of Customer Identification and Verification.* The type of personal information required at account opening varies by service provider with many lacking effective customer identification or record-keeping, “ill-equipped” to verify customer identification or “openly” promoting anonymous payments.
- *Acceptance of Cash and Money Orders.* Acceptance of cash and money orders by currency exchangers facilitates anonymous transactions and shortens law enforcement’s “investigative trail.”
- *Multiple methods used to transfer of value.* Cash, money orders, credit and debit cards and wire transfers used to move value to currency exchangers. Funds transferred to exchangers via money transmitters globally.
- *Criminal Abuses.* Used (a) by operators of Ponzi schemes, (b) to facilitate Internet auction fraud, investment schemes, computer intrusions, and credit and debit card fraud schemes and (c) to launder the proceeds of other criminal activity originating outside the system.
- *Nonrecourse transactions.* All transactions are final, and customers have no recourse if criminals take their digital currency.
- *Lack of consistent or reliable AML policies and procedures.* Due to a lack of clear

<sup>2</sup>Unlike digital currencies, however, the precise financial liability embodied by a virtual currency is often vague as the issuer usually has no current assets specifically reserved buy back or redeem the currency in circulation.

<sup>3</sup>U.S. National Money Laundering Threat Assessment at 25, available at <http://www.ustreas.gov/offices/enforcement/pdf/mlta.pdf>.

regulation, especially across jurisdictions, many online payment systems are not subject to any recordkeeping, reporting or AML compliance program requirements.

In June 2008, after e-gold's indictment and not long before its sentencing, the U.S. Department of Justice's National Drug Intelligence Center (NDIC) issued a report noting that digital currencies are more convenient than other methods of funds transfers because digital currencies are easy to use, transactions can be conducted at any time without regard to geographical boundaries, and they are instantaneous and irreversible.

Elaborating on the Threat Assessment's concerns, the NDIC focused on how unregulated or under-regulated digital currency systems heavily promote themselves as anonymous and unregulated. It noted users of digital currency systems "can anonymously fund digital currency accounts, send those funds (sometimes in unlimited amounts) to other digital currency accounts worldwide, and effectively exchange the funds for foreign currencies — often while bypassing U.S. regulatory oversight."<sup>4</sup>

The FATF issued a similar report shortly thereafter on "Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payments."<sup>5</sup> While the section addressing digital currencies appears to rely solely on the NDIC report and the Threat Assessment, it provided a good summary of red flags and other consid-


erations for evaluating the risks associated with Internet payments generally.

*Are the money laundering or terrorist financing risks for digital currencies more significant than other payment alternatives?* Each new payments innovation presents its own set of unique opportunities and risks of criminal abuse. Predictably, criminals are the first — or among the earliest — adopters of a new payments method, testing how fast, how far and how much value can be created or moved with as little interference as possible for as long as possible. Given the unique characteristics of digital currencies, are they subject to greater criminal abuse than other payments alternatives and thus riskier than other payments alternatives?

Anecdotally, the Threat Assessment reported that law enforcement observed that digital currency systems "have become favorite payment mechanisms for online perpetrators of illegal activity." The NDIC report in 2008 said that digital currencies provide an ideal money laundering instrument." Such comments however do not establish that they are riskier than other payments alternatives.

FATF's 2010 update to its 2006 Report on New Payments Methods<sup>6</sup> reported on its analysis of 33 case studies involving NPMs. It found that "while the analysis of the case studies confirms that to a certain degree NPMs are vulnerable to abuse for money laundering and terrorist financing purposes, the dimension of the threat is difficult to assess." It concluded that money laundering and

terrorist financing risks "can be effectively mitigated by several countermeasures taken by NPM service providers" and suggested that all risks factors and risk mitigants be considered when evaluating the overall risk of a NPM.

Nonetheless, a concern underlying all of these reports is the general lack of regulatory oversight and controls with respect to digital currency systems. Although efforts have been made in the U.S. to provide some formal regulatory guidance for digital currencies, most digital currency systems are based outside the U.S and the U.S.'s ability to reach those operations is limited. The NDIC report stated "it would be nearly impossible to legislate regulatory controls that would allow the U.S. government to prevent completely foreign-based digital currencies from being used in the United States because these services are available through the Internet." 

*Part II of this article will discuss the efforts in the U.S. to regulate digital currencies and what impact that may have on criminal use of such systems. It will focus in particular on the experiences of e-gold, the pioneer in digital currencies, the non-legislative regulation that has been set out for the industry and the lessons of e-gold for other types of emerging payments methods for all AML compliance personnel.*

*Carol R. Van Cleef, CAMS, partner, Law firm Patton Boggs LLP, Washington, D.C., USA, CVanCleeff@PattonBoggs.com*

<sup>4</sup>U.S. Department of Justice, National Drug Intelligence Center, Money Laundering in Digital Currencies at 1 (2008), available at <http://www.justice.gov/ndic/pubs28/28675/28675p.pdf>.  
<sup>5</sup>Financial Action Task Force, Money Laundering and Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems (2008), available at <http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf>.  
<sup>6</sup>Financial Action Task Force, Report on New Payment Methods (2008), [www.fatf-gafi.org/dataoecd/30/47/37627240.pdf](http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf).

## BAM ...Supporting People and Innovative BSA/Fraud Solutions

### BAM: Powerful, Flexible, Affordable

Since 2000, our BSA/AML/Fraud solutions have integrated seamlessly with most major core processors and are easy to incorporate into your existing monitoring program. Want proof? You'll find BAM in the hands of **thousands of satisfied users** at banks and credit unions across the nation. Not only do we support our *solutions*, we support our *customers*.

*"You have a tremendous company and BSA solution set that I am eager to share with colleagues and examiners alike. Thank you for your solution, your partnership, and your support."*

**Jennifer Greger**  
SVP, BSA & Sr. Regulatory Officer  
OMNI BANK - Metairie, LA



CORPORATE OFFICE  
10431 Morado Circle, Suite 300 · Austin, TX 78759 U.S.A.  
Toll Free: (888) 201-2231 · Email: [info@bankerstoolbox.com](mailto:info@bankerstoolbox.com) · [www.bankerstoolbox.com](http://www.bankerstoolbox.com)

# When to make the call to law enforcement

**K**nowing when to file a Currency Transaction Report (CTR) or what documentation is required to open a new account is clearly defined by regulation or company policy. Deciding when to file a Suspicious Activity Report (SAR) is less clear and depends on an AML/CTF professional's knowledge and personal experience to determine when something is not right. But when it comes to going beyond filing a SAR to contacting law enforcement directly, it can be a tough call.

As a compliance officer, you may have struggled with the question of when to reach out to law enforcement and which agency you should call. The following law enforcement experts offer some guidelines to use when faced with these questions.

If you feel the situation threatens irreparable damage, make the call, according to Rick Adams, a retired Special Agent with the IRS Criminal Division. "Call law enforcement if you feel there is going to be harm to the bank; harm to a depositor, for example accountholders wiring money to Nigeria or Canada because they have fallen victim to a lottery scam; or harm to another person, like elder abuse," Adams said. "If you think the situation may cause harm to society, like potential terrorist activity, it should be reported immediately."

Before making the call, take time to assess the risk, Adams advises. If a transaction is just suspicious, like an unusual deposit pattern from one of your known customers, you should report it on a SAR, but not necessarily call law enforcement

Before making the call, take time to assess the risk

"For example, if one of your customers has a video rental company and has had no suspicious activity for two years but now has a huge influx of cash, that's suspicious," Adams said. "But just because it might be unusual and suspicious, the activity isn't over the top."

There are times though when unusual activities can become a pattern of ongoing and escalating suspicious transactions. When that happens, it's time to reach out to law enforcement, according to Al Gillum, CAMS, president of Advanced Compliance Technologies, LLC, and a retired postal inspector.

"Watch the SARs you are filing (on a person or company)," Gillum said. "If you start seeing a pattern over two or three weeks that the dollar values are significant and the activity is an ongoing process, it's time to reach out to law enforcement. A rule of thumb I use is to call at the point the activity is reaching \$50,000."

Jerry Loke, a retired IRS Agent and current member of the Philadelphia Organized Crime and Drug Enforcement Task Force (OCDETF), adds a word of caution. For institutions that don't have contacts within the law enforcement community or for a compliance officer who isn't sure if an activity warrants a call to law enforcement, contacting the local SAR review team might be a better option.

"In extreme situations, like those discussed above, law enforcement needs to be notified, but you do need to put some parameters in place," Loke said. "Otherwise the calls could be overwhelming. Many of the U.S. Attorneys' Offices have district SAR review teams in place. They review SARs weekly and meet once a month to bring SARs before the cross-functional law enforcement team. In situations where you do not have a relationship with a SAR team, it may be best to communicate with the U.S. Attorney's Office directly."

## Who should you call?

Once you decide to contact law enforcement, the next question is who to call. If you have law enforcement contacts, use them. If you don't have contacts, notify the appropriate agency based on the type of crime.

"Determine which agency to call," Adams said. "If it is a terrorist activity, call the FBI. If it involves narcotics call the IRS or the DEA. If you suspect elder abuse, call local law enforcement."

If you don't have law enforcement contacts now, develop them. Every compliance office should have multiple law enforcement contacts, according to Gillum. Build rela-





tionships with law enforcement and draw on them. Partnerships with law enforcement can be a valuable asset to your compliance team.

“Developing a great relationship with law enforcement in your area is critical,” Gillum said. “Every compliance office should have a point of contact with law enforcement. When faced with a situation you are unsure of, call your contacts. You can bounce ideas off of them and ask them what they think of the situation.”

Compliance officers should build strong relationships with both federal and local law enforcement, says Sgt. Jim Cox, CAMS, supervisor of the Special Investigations, Narcotics and Money Laundering Unit of the Fairfax County, Virginia, Police Department.

“I am a firm believer that you should have both,” Cox said. “We get every SAR that involves Fairfax County, but sometimes a


SAR won’t get to us until two years down the road. By the time we get the SAR, we are often already working the case from information we’ve received from the community. Because we are a local law enforcement agency we know the community and get a lot of information from them. The SAR is important and it adds to the case, but the information from the community is also very important. If a teller notices that a guy comes in frequently and visits his safety deposit box and then makes a large cash deposit, we would love get a call on it. If we get a call, we can start working the case.”

#### Making contact

If your list of law enforcement contacts is short, there are a number of ways to enhance it. Call your local police and find out if they have a money laundering unit or financial crimes unit. Find out when they meet and attend the meetings to see what they do.

Attend ACAMS local chapter networking and learning events to meet federal and local law enforcement agents. “Go to the meetings and get to know the people,” Cox said. “Then boom, there are your contacts.”

Also, don’t neglect the resources within your organization. Many financial institutions and money services businesses have retired law enforcement agents on staff. Reach out to them for their knowledge and also ask them for contacts.

“Befriend these people and talk back and forth,” Cox said. “Tell them you’ve filled out a SAR and ask them what they think. Take that extra step, reach out to law enforcement and then let them run.” 

*Debbie Hitzeroth, CAMS, USPS BSA/OFAC compliance officer, U.S. Postal Service, Washington, D.C., U.S.A., [deborah.l.hitzeroth@usps.gov](mailto:deborah.l.hitzeroth@usps.gov)*

# Before – and After – You Start Talking to Law Enforcement

Important tips from the lawyers



Everyone recognizes the importance of cooperating with the law enforcement community and appreciates how even a small bit of information may provide the crucial detail that helps solve a crime or prevent a terrorist act.

However, if you decide to pick up the phone to call law enforcement, you want to ensure that you are not creating any unwanted problems for your institution — and possibly yourself.

For inside advice on how to avoid such consequences, I solicited the views of two of my partners: Ted Planzos who served as an assistant district attorney in Bronx County, N.Y., a special assistant U.S. attorney and the deputy chief of the Organized Crime and Racketeering Section at the U.S. Department of Justice; and Sam Rosenthal, who was a former assistant U.S. attorney and headed the Criminal Appellate Section of the U.S. Department of Justice. Ted recently represented Pamrapo Savings Bank in its negotiations with the Department of Justice and federal regulators. Sam has represented a number of banks and money transmitters in criminal proceedings before federal and state prosecutors.

Here is a list of pointers we developed for your conversations with law enforcement.

- *Circumstances will dictate.* We all agree that your communications with law enforcement will depend on the circumstances, including whether you have information about a customer or one of your employees, whether an investigation has already begun and what the nature of the information is. For example, if the information relates to an unfolding criminal or terrorist act involving bodily harm or destruction of property, you likely will be asked to respond with details more quickly than if the information relates to a prior violation with little or no ongoing significance.
- *Cooperation is the best policy.* The Federal Sentencing Guidelines make clear that full cooperation with law enforcement is a factor considered by prosecutors in charging a corporation with money laundering or aiding or abetting in money laun-

dering. Should an employee be involved or the institution otherwise implicated in the activity, cooperation will be an important mitigating factor for the prosecution and the judge at sentencing.

- *You may be required to call.* Financial institutions should notify law enforcement by telephone if the matter requires immediate attention (you also may be required to call your regulator). The FFIEC BSA/AML Examination Manual states: “for situations requiring immediate attention, in addition to filing a timely SAR, a bank must immediately notify, by telephone, an “appropriate law enforcement authority” and, as necessary, the bank’s primary regulator.”
- *Be brief.* Ted suggests the best strategy is to keep the conversation brief. “You only need to tell the investigators that a SAR filing has been or will be made. They can request the paper.” Sam notes that “any conversation with law enforcement is a significant event whether you call to report concerns about a customer or an employee of the institution. Everything you say becomes evidentiary.” This means that the information you provide law enforcement in a conversation could possibly be used against the institution at a later date.
- *Disclose the SAR if requested and offer it when appropriate.* The new SAR disclosure regulations published in December 2010 generally prohibit the disclosure of a SAR. However, the regulations provide an important exception that permits an institution to disclose to federal, state and local law enforcement that a SAR has been filed or facts that indicate the existence of the SAR as long as the disclosure is not made to a person involved in the suspicious transaction. The new regulation also permits the institution to provide a copy of the SAR to law enforcement.
- *A subpoena may still be required.* The new SAR disclosure regulations make clear that a SAR can be disclosed to law enforcement without a subpoena. However, while the regulations permit disclosure of the underlying facts, transactions and documents upon which

the SAR is based, the regulation does not appear to eliminate the need for a subpoena should law enforcement request the underlying documents.

- *Keep your legal counsel’s number close.* Whether you rely on inside or outside counsel, you should not hesitate to consult with your counsel if you have any doubt about whether you should contact law enforcement or what should be said in the conversation. For example you may consider consulting with counsel as to whether a subpoena is required for the underlying documentation. Ted and Sam also agree that in certain situations where you may want legal counsel to join you on the call. The cost of relying on counsel would easily be offset by much more significant fine/fees or penalties if the proper actions are not taken. A classic “better safe than sorry situation.”
- *Last but not least — don’t forget to file a SAR.* If you have decided the matter was suspicious enough to call law enforcement, it would probably be very difficult to argue that it was not suspicious enough to file a SAR. If you had not decided it was suspicious when you called law enforcement, then a SAR may or may not be required. If law enforcement seems uninterested or explicitly states that the matter is not suspicious, you have a choice. This will be a judgment call. If law enforcement indicates in any way that the information is helpful, or helps to confirm something it is investigating, or will be used to initiate an investigation, you should seriously consider filing a SAR.

These few simple thoughts are intended to help keep the lines of communication between your institution and representatives of the law enforcement community open while protecting the interests of the institution. Your legal counsel may have some additional suggestions for you. 🚓

*Carol R. Van Cleef, CAMS, partner, Law firm Patton Boggs LLP, Washington, D.C., USA, CVanCleaf@PattonBoggs.com*

Have you thought about joining an ACAMS' Chapter lately?  
Come see what all the commotion is about.



## ACAMS Chapters

ACAMS' chapters provide local forums which facilitate discussion, offer educational opportunities focusing on region-specific issues, and foster professional networking among ACAMS members.

## What are the benefits of joining?

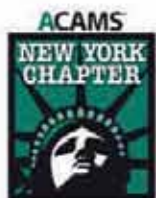
- Learn about money laundering prevention from the most experienced professionals in the industry at workshops designed to help you expand your knowledge in the field both locally and internationally
- Identify and meet other anti-money laundering specialists in your region and explore common interests
- Increase exposure for career advancement
- Join or renew online
- Earn CAMS and CPE credits for attending chapter learning events
- Attend free educational and networking events (more than 75% of these events are free to chapter members)
- Join a local chapter even if you're not yet an ACAMS member

*ACAMS has chapters throughout the world.*

*Don't you think it's time you joined one or started one in your area?*

Visit us at:

[www.acams.org/ACAMS/ACAMS/Communities/Chapters](http://www.acams.org/ACAMS/ACAMS/Communities/Chapters)







# Suspicious Activity Reporting: Quality assurance is key to maximizing reporting value

Reporting suspicious activity to proper governmental authorities is one of the most important ways financial institutions participate in the fight against money laundering and terrorist financing. The laws of most countries have deputized financial institutions, making them vital sources of information and intelligence on the suspicious financial activities of their customers. The suspicious activity report (the term SAR is used in this article, although many other jurisdictions call it by other terms) represents the transfer of this valuable information to law enforcement. If done properly, it will reflect well on the institution, demonstrating how its customer due diligence efforts enabled it to identify the unusual activity and discern that it truly was suspicious and reportable.

However, if the report is not well written, it may result in a failure to convey this vital information. This can reflect poorly on the institution, as well as be the difference between whether or not law enforcement commences an investigation into the suspects and puts a stop to any underlying illegal activities. As the FFIEC BSA/AML Examination Manual states, “a thorough and complete [SAR] may make the difference in determining whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.”

In the United States, several prominent enforcement actions have criticized financial institutions for filing ineffective SARs, both in terms of inadequate reporting, as well as for failing to file SARs in a timely manner. While not all jurisdictions have a deadline by which a report of suspicious activity must be made, the sooner the information can be conveyed to the proper authorities, the sooner appropriate action can be taken to stop illegal activities. Financial institutions should have a means of conducting a review of the timeliness and quality of SARs to demonstrate their commitment to this critical aspect of their AML

programs, as well as their overall efforts to combat crime.

## What is meant by quality reporting?

The term quality has been the subject of numerous guidance documents published by various regulatory agencies. The common themes in defining the term quality include completeness, accuracy and timeliness of the report. So what really separates a merely accurate SAR from a quality SAR? Accuracy of the information in the report should be considered a minimum standard. All information being filed should be error free and as complete as possible. It is essential for the preparer to ensure the accuracy and the completeness of the reporting fields prior to formal filing. Inaccurate information could delay a criminal law enforcement case due to the inability to identify the right suspect or potential target. Further, filing a SAR with incorrect information, such as an inaccurate personal identifier, could require the financial institution to file a corrected or amended report, which pulls resources away from current workloads to correct an item that should have been prevented initially.

In addition to the accuracy of information, a quality report should detail all available information from the financial institution’s perspective and formulate the narrative in such a way that is logical and detailed. The financial institution knows a significant amount of information about the customer that may not be readily evident to a law enforcement official investigating the customer. The person preparing the report should take great care in the narrative preparation and adequately describe the persons and events associated with the activity. Another guiding principal in writing a standard narrative should be to follow the 5 “W’s”: *who* is conducting the activity and who is involved in the activity; *what* are the transactions involved (including types of transactions and the values of the transactions); *where* were the transactions conducted; *when* were the transactions conducted and perhaps most importantly,

*why* does the institution consider the activity suspicious. The narrative should also describe *how* the suspicious activity occurred, clearly showing how the suspect transactions or patterns of transactions were committed. The preparer should place in the narrative all facts learned during the analysis of the activity, even if the fact appears to be trivial in nature.

## Forming a quality assurance process

Quality and accuracy are the responsibility of anyone who reviews a draft of a SAR prior to the formal filing of the report. The filing of a SAR and the determination of suspicious activity are generally the responsibility of an investigations group. The report’s preparer has a primary accountability to ensure that the data being reported is accurate and error free. The preparer also is the person within the institution who understands the totality of the suspicious activity, including any related parties. The institution should implement a process whereby a team leader or senior manager reviews draft SARs before filing. The reviewer, who is not as familiar with the suspicious activity as the preparer, can conduct an independent review of the SAR to determine whether it makes sense and clearly explains the unusual activity being reported. The reviewer, as a member of the investigations group, also has a vested interest in the accuracy and quality of the information presented in the draft SAR, as this impacts directly on the unit’s productivity. This is the opportune time to make any changes or edits to the information contained in the draft. Taking this extra step will help prevent filing errors and additional work by the institution.

Financial institutions can take the evaluation of SAR quality to another level by the formation of an independent team of Quality Assurance analysts that reviews the SARs after filing. While it may be customary for pre-filing reviews to be done by team leaders or senior managers within a centralized investigations or financial intelligence group, a secondary review group outside of the centralized SAR filing group is an independent group that can

provide a wealth of information for senior management. This secondary group's focus is to review the SARs filed and validate the information reported against the information contained in the institution's customer and account systems.

The independent SAR QA group may have its own procedures and scoring methodologies in place to properly evaluate the SAR filings by group or even by individual. The SAR QA group is an additional layer to determine accuracy, completion and timeliness of the SAR. Since the decision to file a SAR is often a subjective determination, the SAR QA group is generally not focused on determining whether or not the decision to file a SAR was warranted. However, it should consider reviewing determinations by the investigations group that a SAR is not warranted to determine that the investigations unit is adequately documenting these decisions.

Both the independent SAR QA group and the investigations reviewers can also provide some internal filing trends and identify patterns of SAR filings that may be of importance to senior management. The review teams also facilitate the identification of specific errors by particular preparers, enabling the institution to tailor refresher training to correct the issue and prevent future errors. The tracking of SAR quality by preparers can also be used as a barometer of individual and team performance during regularly scheduled personnel reviews. The function can also help resolve matters prior to a formal audit or regulatory exam.

### Impacts of poor quality SARs

There are a number of significant impacts of poor quality SARs. While implementing a SAR QA process entails expending a fair amount of resources in terms of dedicated staff time, the costs outweigh the adverse consequences. Poor quality SARs can result in revisions or amended filings, which, if these occur frequently, can result in a less than satisfactory examination by regulators, who likely will see a deeply flawed process. While some systems may have automated controls that assess whether or not information is contained within the required reporting fields, these often are not able to assess the quality or accuracy of the information, two aspects that can lead to amended filings. As with any less than satisfactory examination, an institution will be required to spend a significant amount of resources to repair the deficiency — often by implementing a SAR QA function that should have been in place. Further,

continuous filing errors in SARs can result in monetary fines by the regulators, which can lead to reputational damage should the settlements be made public.

However, outside of the direct impact to the institution, a poor quality SAR can lead to a delay in investigating potentially criminal activity. For example, if an institution does not provide accurate information, it could prevent law enforcement from investigating the correct suspect. If an institution does not convey the correct account information, it could result in law enforcement issuing a subpoena for incorrect information, which could result in an embarrassing situation should the institution return the subpoena with information that there is no such account on its books or information that is not related to the underlying unusual activity. Law enforcement will often review the SARs submitted to determine if there is sufficient basis for conducting an investigation into potential criminal activity. If an institution's SAR does not provide sufficient explanation for why the activity is suspicious, law enforcement may not even initiate an investigation. This last scenario must be one of the most frustrating outcomes of SAR filing — that all the investigative effort expended by the institution leads to nothing more than noise in the system, while the criminal activity continues. Further, poor quality SARs can also divert law enforcement's limited resources by causing them to follow up with institutions to obtain information that should have been included in the original report.

A poorly prepared SAR could impact law enforcement's ability to identify and track a pattern of activity for a potential money launderer or terrorist group. This in turn has an impact on the financial well being, as well as the security of the community the institution serves and where its clients and employees live.


### Feedback from law enforcement

Law enforcement and government regulatory agencies have noted that quality SAR information has led to the investigation and conviction of criminals and associated parties. Reinforcing the point that the SAR represents the most important link between an institution's AML program and law enforcement, a quality SAR clearly shows law enforcement what the institution has observed, why it is unusual and gives them the information they need to follow up and further investigate the unusual activity.

Law enforcement officials are generally not as well trained in analyzing financial transactions as institutions' AML investigators; particularly not with regard to how to navigate the institution's systems to follow the money trail. Thus, it is through the SAR that the institution is able to articulate the flow of funds, which is exactly what law enforcement needs to trace the criminal activity they can detect — and which is generally their responsibility to determine — to the funds they need to confiscate from the criminals.

Over the years, investigators at our institution have received numerous commendations from law enforcement citing how the information we provided enabled law enforcement to follow complicated and sophisticated mazes of transactions designed to obscure the trail of funds and bring criminals to justice and to seize funds that could be used to compensate victims of the crimes. In fact, the number of these commendations has increased as a result of implementing the SAR QA process. These commendations have been a huge boost in morale to our investigators, leading to increased productivity, as well as fostering a stronger working relationship between the institution's investigators and law enforcement.

### Conclusion

The SAR is one of the most important ways an institution's AML program actually combats the crimes that underlie money laundering and terrorist financing. As such, it is one of the most important contributions financial institutions can make to the communities they serve. While any form of tips can help, poor quality SARs will generally not lead to investigations and may sap resources that could be used to pursue criminal activity. Quality SARs are the ones that will lead to significant improvements in the way law enforcement is able to use the intelligence institutions provide them on suspicious activity. A process designed to assure quality in every SAR helps maximize the value and utility of the institution's SARs, demonstrates its commitment to fighting money laundering and terrorist financing, minimizes unnecessary rework and creates a strong partnership with law enforcement. 

*Melissa Morelli, CAMS, vice president, Bank of America, Charlotte, NC USA, [Melissa.l.morelli@bankofamerica.com](mailto:Melissa.l.morelli@bankofamerica.com)*

*Kevin M. Anderson, CAMS, director, Bank of America, Falls Church, VA, USA, [Kevin.m.anderson@bankofamerica.com](mailto:Kevin.m.anderson@bankofamerica.com)*



# Federal Register

## —The daily journal of the U.S. government

Ladies and gentlemen allow me to introduce you to the Federal Register. Already aware of its amazing powers? Then this article might not be for you. If, however, you have read the same regulation again and again but still wrestle with its meaning, or need to truly understand the thought process behind a particular rule, then the Register is your place.

First let me provide a little background. A bill, such as the Bank Secrecy Act (BSA), after the legislative and executive process, becomes a law or act. A law/act can be self-executing, meaning no regulations are required prior to publication, or in the contrary a law/act can require the publication of regulations.

Regulations explain how the law will be applied or interpreted. Before publishing regulations however, the responsible agency or responsible department will issue proposed rules. These proposals are commented on by members of the industry impacted by the Act. The agency will review the comments, discuss reasons for incorporating or rejecting said comments and eventually publish final regulations. This give and take between the industry and the regulatory agency is captured in the Federal Registry and it is this 'give and take' that can be valuable.

Below is an example of one benefit of the Federal Register.

Section 5318 (i) of the BSA requires due diligence for United States Private Banking and Correspondent Bank Accounts Involving Foreign Persons. Going somewhat further 5318(i)(3) states that ... *at a minimum, ... the financial institution takes reasonable steps (A) to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, such account...*

The BSA requires that reasonable steps be taken to ascertain the source of funds deposited into a Private Bank account involving Foreign Persons. The task may seem daunting and perhaps impossible when you consider things like the volume of transactions in an account and the obstacles posed by verifying almost any information. By simply restating the BSA, the Regulations, specifically 31 CFR 103.178 (b)(2), offer little insight. The Federal Register, however, provides helpful language in determining how to turn language of the BSA into an understandable reality.

*"... we do not expect covered financial institutions, in the ordinary course, to verify the source of every deposit placed into every private banking account. However they should monitor deposits and transactions as necessary to ensure that the activity is consistent with information the institution has received about the client's source of funds and with the stated purpose and expected use of the account, as needed to guard against money laundering, and to report any suspicious activity."* (Federal Register, Vol. 71, No. 2/Wednesday, January 4, 2006/Rules and Regulations, Page 509).

It is only after reading the relevant Federal Register sections that one can begin to conceptualize how to comply with the BSA. In this situation financial institutions are not required to verify the source of every deposit — clear and simple.

Here is an example of a helpful 'give and take.'

Section 3518 (i) (3) (A) of the BSA requires financial institutions (A) to ascertain the identity of the nominal and beneficial owners. In the Regulations a beneficial owner of an account *means an individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a*



*practical matter, enables the individual, directly or indirectly to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however, without any corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner.* 31 CFR §103.175 (b).

The originally proposed rule was different. It used the term Beneficial Owner Interest which implied that almost anyone who had access to the account would fall under the "identify" requirement. There is also a minimum dollar amount of interest, but it is not relevant for this discussion. Problems with the originally proposed rule were addressed through various comments.






*“...the Associations believe that the definition of “beneficial ownership interest” is overly broad. A possible approach could be that the final rule would not seek to define “beneficial ownership interest” with general terminology, but rather allow covered financial institutions to determine which persons, in particular circumstances, should be viewed as having the requisite beneficial ownership. The requisite beneficial ownership could be determined by reference to that level of ownership that, as a practical matter, equates with control over or entitlement to the account...”* (Joint Letter from: ABA Securities Association American Bankers Association Bankers Association for Finance and Trade Financial Services Roundtable Futures Industry Association — July 1, 2001).

The arguments were persuasive and the definition was narrowed. The Register goes on to explain, *“The Rule also should provide covered financial institutions with a workable standard for assessing beneficial ownership for private banking accounts, thereby allowing covered financial institutions to focus their due diligence efforts in a risk-based fashion on those accounts and individuals posing a heightened risk of money laundering.”* (Federal Register/Vol. 71, No. 2/Wednesday, January 4, 2006, Rules and Regulations. P 505).

In the end, the thing to remember is to focus your due diligence efforts in a risk-based fashion on those accounts and individuals posing a heightened risk of money laundering. Thank you Federal Register!

To be clear, the Federal Register is not the only place for guidance. The FFIEC manual also provides a tremendous amount of information. Remember, however, that the writers of the FFIEC Manual review and are persuaded by the contents of the Register. The “source of funds” discussion above is a good example. The FFIEC guidance is very similar to what is written in the Register. See FFIEC Manual 2010, page 132.

So when nothing else matters but a clear understanding of the BSA go to <http://www.regulations.gov> or <http://www.fincen.gov>. Both are easily navigable sites that provide access to the BSA and the Regulations. 

*Michael Kneis, CAMS, HIFCA, El Dorado Task Force/ HIDTA, New York, NY, USA, [mkneis@nynjihidta.org](mailto:mkneis@nynjihidta.org)*



# Viewing in monochrome?



I have been blessed throughout my 38-year professional career to be associated with truly outstanding professionals. I spent 31 years in government service, 28 with the Federal Bureau of Investigation. The integrity and dedication I encountered among my law enforcement peers was noteworthy. I was extremely proud of my friendships and associations. Over the last seven years as a consultant working with compliance and fraud specialists, I have had the privilege of observing the same levels of integrity and dedication. I have likewise been proud of the friendships and associations I have developed in the private sector.

The primary difference between my law enforcement and private sector colleagues is perspective. Not many people recognize this important fact. Both my law enforcement and private sector contemporaries understand the importance of partnering with each other. Unfortunately, successful partnerships have been on a one-off basis and not systemic and sustainable. One reason for this is the difference in perspectives.

Many of the individuals I have had the honor to associate with in law enforcement and the private sector are innovative thinkers. However, in most instances, they have been unable to affect institutional innovation. Law enforcement and private sector institutions tend to operate in their safety zones, and frequently, innovation falls outside the institutional safety zone. As a result, there is little incentive to develop innovative techniques to fight fraud and money laundering.

This brings me to the point of this article: perspectives, partnerships and innovation.

## Introduction

When it comes to fraud and money laundering, the bad guys are not constrained by boundaries. This affords them the opportunity to be proactive and imaginative in furtherance of their illicit activities. In fact, the more proactive and innovative the bad guys become, the more incentive they derive. Conversely, law enforcement and the financial services sector are frequently constrained by red tape and reluctance to implement change. Regulations, privacy considerations, policies, procedures, budgetary constraints and a myriad of other factors often serve as impediments to proactive measures and forward thinking. Regulations are such that reactive transaction monitoring and fraud detection in the financial services sector is the accepted norm. There is little incentive

for innovation. Consequently, the bad guys have a considerable advantage.

As we have witnessed in the last few years, corporate frauds, investment frauds and mortgage frauds have devastated our economy. Add to that the continuous stream of check fraud, loan fraud and credit card fraud, not to mention health care fraud, and other crimes, and our economic problems are significantly compounded. The one constant in the various fraud schemes we have experienced is the ongoing need to launder these criminal proceeds. The intersection of fraud and money laundering should be the focal point for prevention and deterrence.

The time has come to take the advantage away from the bad guys in a sustainable and meaningful way. To achieve this, law enforcement and the financial services sector must first truly understand, embrace and act upon three words: perspectives, partnerships and innovation.

## Perspectives

In many of the training presentations I have given since I retired from the FBI, I have commented that when I retired and became a consultant, I thought I knew everything I needed to know about bank anti-money laundering (AML) and fraud compliance and investigations. What I came to realize in a heartbeat was how little I actually understood about the AML compliance and investigative function. It was not a matter of not knowing, it was a matter of not understanding the financial institution compliance and fraud perspective. That was a humbling and educational experience. Over the last seven years, I have worked hard to understand and appreciate the financial institution perspective. For the benefit of my law enforcement friends, if I knew then (when I was in law enforcement) what I know now, I would have been dangerous. I encourage my law enforcement colleagues to learn from my experience and look beyond your perspectives when dealing with the private sector.

The reality is that many law enforcement officers do not understand the perspective of the bank compliance or fraud specialist. Likewise, many bank compliance and fraud specialists do not understand the perspective of the law enforcement officer. The first step in progressing to sustainable and meaningful partnerships is for the two sides to understand and respect the differences in perspectives.

The fundamental difference in perspectives is that law enforcement is driven by criminal investigations. They must focus on developing evidence to support criminal prosecutions. Bank investigators focus on identifying and reporting suspicious activity. These two focuses would appear compatible; however, in between law enforcement and the banks sit the regulators. Without assessing blame to anyone, the regulatory system is such that the banks have to satisfy the regulators before supporting law enforcement. This is where the greatest strain on understanding perspective exists. Law enforcement is focused on their criminal case. They generally do not understand the banks' dilemma in having to satisfy regulators when there are bad guys to put in jail. In the meantime, banks are not necessarily concerned about whether the bad guys go to jail. They are concerned about getting the bad guys out of their banks and how the regulators will respond. Exacerbating the problem is the fact that although regulations and laws are written in black and white, their implementation and interpretation are gray and subjective.

Law enforcement and financial institutions need to address the conflict in their respective perspectives and understand that each possesses information that would greatly benefit the other. Law enforcement has investigative and intelligence information regarding schemes and trends. I frequently hear complaints and frustrations expressed by bank compliance and investigative specialists that law enforcement does not share such information. Conversely, banks contain an incredible repository of financial information and intelligence that would greatly enhance criminal investigations if law enforcement was aware of its existence or where to obtain it.

Law enforcement and financial institutions must come to terms with perspectives. Once that is achieved, the foundation will be set for more productive partnerships. Such partnerships will be better positioned to be sustainable and meaningful.

## Partnerships

There have been a number of public and private partnerships that have achieved success. Most of these have been at the local or grass roots level. We need to develop more robust partnerships at both the grass roots and, more specifically, at the national level. The starting point should be with the realization that both law enforcement and financial



institutions share the mutual responsibility to safeguard our financial system and their customers from fraud and money laundering.

One way to accomplish this is to develop crime problem specific partnerships. In doing so, law enforcement should develop case typologies specific to the crime problem and how the finances of the criminal activity flow through financial institutions. By sharing these case typologies and trend analysis information with the private sector, law enforcement will enable the private sector to more effectively and efficiently identify and report suspicious activity. By doing so, both sides benefit. Law enforcement develops evidence to support criminal prosecutions and/or, asset forfeiture and recovery. Financial institutions in turn will reduce institutional risk.

There is a great example of a public-private partnership that is crime problem specific and typologies driven. It was initiated by JPMorgan Chase (JPMC) under the leadership of William Langford. In 2009, JPMC Corporate AML founded a team dedicated to identifying and assessing immediate and strategic risks to JPMC. This outstanding team enthusiastically developed an issue-based approach by which they identified specific crime problems that presented them with significant risk. In 2010, JPMC identified human trafficking as a significant crime problem and a vehicle for institutional risk. Overall, the project developed typology based surveillance models and investigator training to better enable the identification of potential human trafficking. JPMC's team of dedicated compliance and investigative professionals meticulously developed typologies which enabled them to identify transactional activity associated with human trafficking.

The next step was to develop active channels for coordination with relevant law enforcement agencies, especially those specifically focused on human trafficking. William and his team formed an outstanding working partnership with Immigration and Customs Enforcement (ICE), who have a dedicated group of agents assigned to investigate human trafficking. Through two way information sharing, JPMC was able to identify additional typologies while ICE was able to develop evidence to sustain criminal prosecutions.

Human trafficking is a heinous crime problem. The meaningful partnership formed by JPMC and ICE has begun to grow. In

September 2010, during the annual ACAMS Conference, ACAMS executive vice president John Byrne hosted an informal, off the record meeting between law enforcement and members of the ACAMS Advisory Board to discuss how ACAMS could facilitate partnerships between law enforcement and the financial services sector. Among some promising takeaways from that meeting came a subsequent meeting in Washington, D.C., between Byrne, advisory board chairman Rick Small, board member William Langford and senior executives at ICE. One of the topics was human trafficking.

The industry needs to be less predictable in transactional monitoring and more targeted and proactive

Because of the devastating impact of this crime problem on its victims, ACAMS has formed a Human Trafficking Task Force, which Langford will chair. This initiative will provide a platform for the public-private partnership started by JPMC with ICE to grow and become more sustainable. In furtherance of this effort, on January 13, 2011, ACAMS hosted a free webinar training session on human trafficking. Byrne served as moderator along with ICE agent Angie Salazar, who provided a compelling training session. Education and training promote awareness, which frequently leads to action.

In establishing the issues based approach, JPMC did not settle for a traditional or reactive transaction monitoring framework. Langford and his team took an innovative and proactive approach to dealing with challenging crime problems. It should be noted that JPMC is not alone in developing innovative approaches to identifying and reporting suspicious activity. JPMC represents but one example of how certain financial institutions are gravitating toward the use of more proactive mechanisms.

### Innovation

Langford's team conducted extensive research to develop typologies. They relied


on data mining and proactive targeted model development. By being proactive and focused, JPMC more effectively and efficiently identified suspicious activity consistent with human trafficking. The methodology developed by JPMC should serve as a model for future transaction monitoring models.

The industry needs to be less predictable in transactional monitoring and more targeted and proactive. There needs to be a balance between traditional reactive transaction monitoring and crime problem specific proactive targeted monitoring. A balanced approach between reactive and proactive monitoring would keep the bad guys off balance in their efforts to exploit areas of risk vulnerability.

A challenge going forward with this approach is incentive. The incentive for JPMC was doing the right thing. In terms of tangible incentives for financial institutions to implement similar typologies and methodologies, there is little. This is where the regulators could be a factor. If there was a regulatory incentive to develop crime problem specific monitoring typologies and proactive techniques, the more financial institutions would be inclined to develop programs similar to JPMC's. This would significantly increase the generation of more consequential suspicious activity reports.

JPMC has applied the issues based approach to other significant crime problems. Hopefully, as they reach out to the relevant law enforcement agencies to form partnerships, those agencies will respond as well as ICE did to human trafficking. Building meaningful and sustainable public-private partnerships is the best way to take the advantage away from the bad guys.

### Conclusion

Since the bad guys are not constrained by boundaries when it comes to fraud and money laundering, it is incumbent that law enforcement and the financial services sector share the responsibility to contain and disrupt their criminal activity. The more proactive and coordinated law enforcement and industry are the more likely they are to deter the bad guys. The combination of perspectives, partnerships and innovation will provide the framework needed to stem the tide of fraud and money laundering. 

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

Pre-Conference Training: September 18, 2011

Main Conference: September 19-21, 2011

**ARIA • LAS VEGAS**

**ACAMS Members  
pay only \$1245\*!**

Register by May 31, 2011 with  
VIP code ACAMS-1245

ACAMS 10th Annual International  
**Anti-Money Laundering  
CONFERENCE**

**Reserve your seat today!**

- ▶ Three days of non-stop education offering the most valuable and comprehensive AML/CTF training available
- ▶ Learn from the experts in over 50 unique sessions addressing your toughest compliance challenges
- ▶ Expand your network to include AML executives from around the globe



Presented by

Association of Certified  
Anti-Money Laundering  
Specialists®

**ACAMS®**

Register now! \* • [info@acams.org](mailto:info@acams.org) • +1 305.373.0020

[acamsglobal.org](http://acamsglobal.org)

**MEDIA PARTNERS:** **ML** MONEY  
LAUNDERING.COM

**CA** COMPLIANCE  
ADVANTAGE.COM

\* Use VIP code ACAMS-1245 for this special offer. Register and submit payment by May 31, 2011 and pay only \$1245 for the main conference after ACAMS Member early registration discount is applied. Pre-conference workshops are not included in main conference pricing. Special discounts are available for groups of 3 or more and government agencies. Please contact ACAMS for details. Offers cannot be combined.

# AML risk assessments

## – Concepts and methodologies to fully understand a financial institution's risk

Money Laundering (ML) and Terrorist Financing (TF) are global issues crossing each and every border with a large impact on the financial services sector. Do you know and understand this impact on your financial institution? Can you explain where your ML and TF risk lie? International mitigation efforts have been put in place in attempts to intercept and combat both ML and TF activity. The Financial Action Task Force (FATF) recommendations have been passed down to country Financial Intelligence Units, such as AUSTRAC, FINTRAC, FIC, JFIU, and FinCEN to name a few. These recommendations cover expectations of what an anti-money laundering (AML)/counter terrorist financing (CTF) program should have in place. In addition, FATF's Inter-pretive Note on the Risk Based Approach (IN-RBA) mandates financial institutions to perform AML/CTF Risk Assessments. When assessing a financial institution's risk, these recommendations should be addressed and risk assessed accordingly. Within the United States, guidance on risk assessments given through the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual. Moreover, financial institutions should follow guidance as offered by their country's FIU, regulator or ministry of finance.

AML and CTF risk assessment should be the driving force of a financial institution's AML/CTF compliance program, identifying key areas for potential money laundering and terrorist financing activity. The foundation of a sound AML compliance program lies within a thorough AML risk assessment.

When assessing risk, it is important to remember some areas within the financial services industry pose a greater risk for potential money laundering and terrorist financing than other areas, due to the inherent nature of the business and transaction types involved. These areas of higher risk deserve a higher level of attention and must be afforded

more scrutiny within the risk assessment process. Areas within a financial institution with little or no AML or CTF risk should be allocated the appropriate attention.

### AML risk assessment foundation

Understanding that not one size fits all and that no one approach or methodology is absolute, the foundation for an effective AML risk assessment should include, at minimum, the following risk factors:

- Client types banked
- Products and services offered
- Geographical reach

A financial institution's client base should be examined. As high-risk clients carry with them a greater risk for potential money laundering and terrorist financing, greater scrutiny should be given to Money Services Businesses (MSBs), Politically Exposed Persons (PEPs), Embassy and Foreign Consulate (EFC) and Private Investment Companies (PICs) accounts, to name a few. These client types should be identified and risk rated accordingly. In addition, all high-risk client-types as defined by a financial institution should be considered and risk rated as well.

The number of high-risk products and services offered by a financial institution directly correlates to the institution's AML and CTF risk. Along with products and services offered, transaction processing should be examined as well. The number of wire transfers, for example, should be identified, analyzed and assessed within the risk assessment. These transactions include both domestic and international cross-border wire transfers. Additionally, domestic ACH and International ACH Transactions (IAT) should be given the same scrutiny as wire transfers. Further, it is recommended to consider taking a hard look at any new product initiatives or products and services that have recently become 'hot topics' within the industry such as Remote Deposit Capture (RDC), Third Party Payment Proces-

A qualitative and quantitative approach to a risk assessment collectively makes for a more accurate and reasonable assessment of risk

sors (TPPP), Bulk Shipment of Currency (BSC) as well as previously mentioned IAT. It is equally important to consider evolving and emerging product types such as electronic money movements and mobile payments as these product types tend to be conduits for potential money launderers or terrorist financiers as controls and mitigations may still be in the development phase.

A financial institution's footprint, its presence in regions known for drug trafficking and/or financial crimes, as well as overseas exposure, plays a major role in the assessment of AML/CTF risk. Equally important, it is imperative to assess a financial institution's exposure to high-risk countries, conflict countries, and those countries or regions in which its government has placed sanctions or boycotts.

The size and complexity of an institution may play a factor in assessing a financial institution's AML and CTF risk. Larger, complex financial institutions with an international footprint may wish to assess their risk at a business unit level. Keeping in mind that regulators are requiring an enterprise-wide AML risk assessment, a business unit risk score roll-up would be a viable option within this approach. Smaller, less complex finan-





cial institutions may wish to assess their risk on a corporate level only. Regardless of the approach, the final risk assessment must encompass an enterprise assessment of AML and CTF risk. The important element to remember is that there is not one approach that is necessarily correct.

A three-pronged approach is recommended in the development of a financial institution's AML risk assessment:

**Phase 1 — Information gathering and inherent risk**

The first phase of developing the AML risk assessment is information gathering. A complete inventory of a financial institution's client-base, products and services offered and geographical locations must be taken prior to evaluating the institution's risk. A

solid understanding of client base, the types of transactions they utilize and the volumes of transactions processed must be established. A financial institution's geographical presence, foreign exposure and assets under management should also be collected and gathered. Once you have drawn a map of the financial institution's footprint, created a list of products and services offered, and identified who the clients are, one now has the knowledge and tools necessary to effectively assess the financial institution's AML and CTF inherent risk.

A recommended methodology for uncovering and analyzing a financial institution's inherent risk is in two parts. First, survey or interview those business units within a financial institution that have been identified as having applicability for AML or CTF risk.

Make sure to engage the appropriate business unit managers, compliance officers, and subject-matter experts responsible for AML and CTF risk mitigation and the knowledge to effectively answer and explain their business unit profile. These individuals should be able to speak about client-base, products and services offered, as well as their business unit's geographical footprint and international reach.

Second, request corporate management information systems (MIS) data reports to quantify dollar amounts, transaction volumes and number of accounts around each individual risk factor. These reports can serve as supporting documentation to what has been uncovered through the business unit interview or survey. This leads to both a qualita-

tive survey analysis as well as a quantitative data review.

When assessing risk and looking at transactions, be sure to understand where the transactions take place, who has ownership for control and risk mitigation. This transfer or shared risk concept includes, but is not limited to, back office support business units and business units that serve as product or service delivery channels. It is important to accurately and effectively assign and allocate risk. In many cases, a business unit may own a customer relationship. However, the transaction or service may be offered or serviced within another business unit.

Support business units often have client contact and in many cases transact business by request of and for the benefit of a client. Client-owning business units are not always responsible or aware of products or services being utilized by their clients because they are provided by another channel. As a result, product and service risk must be appropriately assigned to the appropriate delivery channel responsible for the transaction or service. This methodology transfers risk from the business unit owning the client relationship to the business unit that actually processes a transaction on behalf of or for the benefit of a client. Within these cases, risk mitigation belongs to the business unit responsible for the process.

### Phase 2 — Risk mitigation and control assessment

The second phase of developing a financial institution's AML risk assessment is the explanation of risk mitigating controls to defend against illegal activities. These controls include policies and procedures, transaction and account monitoring, investigative units and training programs. Now is the time to make mention of any controls the financial institution has put in place to mitigate its money laundering and terrorist financing risk. AML and CTF controls are an important factor to assessing a financial institution's risk. Although many areas of banking and financial services may be inherently risky when speaking of money laundering or terrorist financing, risk mitigating controls properly put in place may help to offset such risk, thus lowering the level of risk within that area of service.

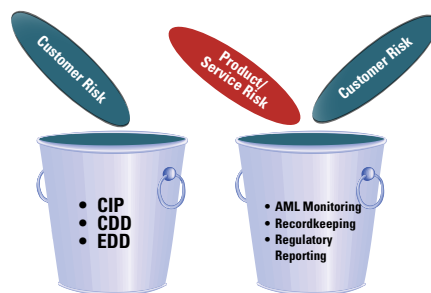
An effective AML program should include the following risk response strategies or risk components:

The risk assessment is a living and breathing document. It must be adaptable to the changes and complexities of AML and CTF risk

- Client Identification Program (CIP)
- Client Due Diligence (CDD)
- Enhanced Due Diligence (EDD)
- AML Policy and Program Governance
- AML Transaction Monitoring and Investigation (FIU)
- Country or Region Sanction Laws and Boycotts (OFAC)
- Regulatory Reporting (SAR) (STR)
- Record Retention and Record Keeping

In addition to the above referenced compliance responsibilities, product, service and customer risk must be monitored and risk rated as well. A recommended approach and methodology is to map these risk factors and consolidate into risk components or risk response strategies (see figure 1). This allows for an assessment of these risk factors at a component level and makes for a more easily understood risk analysis. As processes and procedures are generally constant for each client type, product or service, it would be

Figure 1  
Mapping Risk Factor to Risk Component



redundant to show CIP, CDD and EDD for each of your client-types banked. It makes better sense to consolidate all client-types into one grouping and risk rate accordingly.

Utilizing the risk factor mapping methodology allows for the ability to assess both inherent and residual risk at a component level. A roll-up of products, services and client-types into the appropriate component allows for one inherent risk rating for multiple risk factors. Once inherent risk has been identified for each component, a review of the policies, procedures and controls will help to assign a residual risk rating for each component. Depending on the effectiveness of these control, risk reduction points are assigned. Controls may be found to be effective, marginally effective or ineffective, which demonstrates the number of risk reduction points assigned, if any. As a result, the inherent risk rating score minus the risk reduction points assigned equates to a final residual risk rating.

### Phase 3 — Gap analysis and action plans

The third and final phase of developing a financial institution's AML risk assessment is to identify areas of exposure and possible gaps in which potential money laundering or terrorist financing may find the cracks and leak through. This gap analysis is crucial to uncovering areas that need heightened scrutiny and tighter controls. It is important to remember that the AML risk assessment should drive the AML compliance program. It is the second phase of your AML risk assessment that you begin to make your assessment actionable. By doing so, you begin to amend or draft policies, procedures, processes and controls around those areas identified as having potential risk for money laundering and terrorist financing. The level of risk identified within these gaps determines the level of due diligence required. Should the risk so warrant, an action plan may be put into place to mitigate risk and close this gap.

### Risk rating and scoring

When establishing a scoring criteria or risk rating methodology, the starting point of the scoring matrix should begin with risk rating scores of low to high. Assigning numbers to each risk rating variable helps to simplify the sum of the overall enterprise risk rating score. When assigning numbers and weights to the risk rating variables, sometimes a simple equation is better.

Five Point Scoring Scale Example (figure 2)

- May be either Alpha (Low to High), (Minimal to Extreme) or Numeric (1 – 5)
- Color Coding is also recommended
- Important to include Not Applicable (NA) as this shows risk was not overlooked and scored

Figure 2

Risk Rating		
Low	L	1
Low / Moderate	L/M	2
Moderate	M	3
Moderate / High	M/H	4
High	H	5
Not Applicable		

Putting it all together

Should the risk assessment be conducted at a business unit level, each business unit should be assigned the applicable components and risk assessed accordingly. Alternatively, one may utilize this same approach at a business segment level or corporate level, given the size and complexity of a financial institution. However, if a financial institution warrants a business unit or business segment level assessment, it is recommended to create an enterprise level view of all business units assessed with an overall corporate risk rating. A consolidated view of all business units assessed affords corporate governance with an enterprise view of where risks lie. Additionally, such a view targets business units with multiple risk factors in relation to other business units. This may warrant additional focus for those business units.

The AML compliance program and AML risk assessment should work together. This is the opportunity to assess a financial institution's AML and CTF risk and tighten controls where needed. The assessment of these risks becomes the foundation for establishing a successful AML compliance program. A financial institution's AML risk assessment should serve as an umbrella of the AML compliance program. Moreover, it may also be utilized as a reference manual that quickly identifies a financial institution's risk exposure, as well as to serve as a quick reference to where products and services are being offered, what business unit are banking high-risk clients, and what the geographical

footprint looks like, among other relevant corporate profile information.

Throughout the AML risk assessment, offer an explanation of any AML or CTF risks present and controls put in place mitigating such risks. A well thought out commentary and supporting language to address the risks and controls surrounding those risks helps regulatory examiners understand the business, the corporation and its AML compliance program initiative. In addition, this same approach offers a high-level executive summary for internal executive management as well as the firm's chief BSA officer or AML director. Further, reference any materials used in the information gathering stage. Document what has been found and attach or footnote reference materials. A clear explanation of risk supported with documentation of findings makes for an easily understood document for its readers.

The AML risk assessment should reach a conclusion. The assessment should identify the level of AML and CTF risk present within



a financial institution as well as to assign a final risk rating score. The final risk rating score should identify a financial institution's inherent and residual risk ratings and vulnerabilities of being used to launder money from illegal activities or conduct terrorist financing. In addition, offer an explanation of the scoring criteria. If numeric values have been assigned to identify levels of risk or if one factor was weighted more heavily than others, explain it.

Once the AML risk assessment has been completed, put it into action and make it usable. The AML Risk Assessment should be a working document. At minimum, an

assessment of AML and CTF risk should take place every 18 months or annually for larger financial institutions. Risks need to be reevaluated as the business changes. Changes within a financial institution must be accompanied by a commensurate change in the AML Risk Assessment. As a result of the fast paced environment of the financial services industry, the AML risk assessment has a limited life expectancy. It should be reviewed as circumstances dictate and keep pace with the changes and complexities of AML and CTF risk.

The risk assessment is a living and breathing document. It must be adaptable to the changes and complexities of AML and CTF risk.

Conclusion and communications

Results from the AML risk assessment will assist in the evolution of the AML compliance program. It will provide inputs for planning and prioritization within areas such as:

- Business unit procedural enhancements
- Planning for controls and testing scope and coverage
- Training opportunities
- Additional or enhanced transaction monitoring

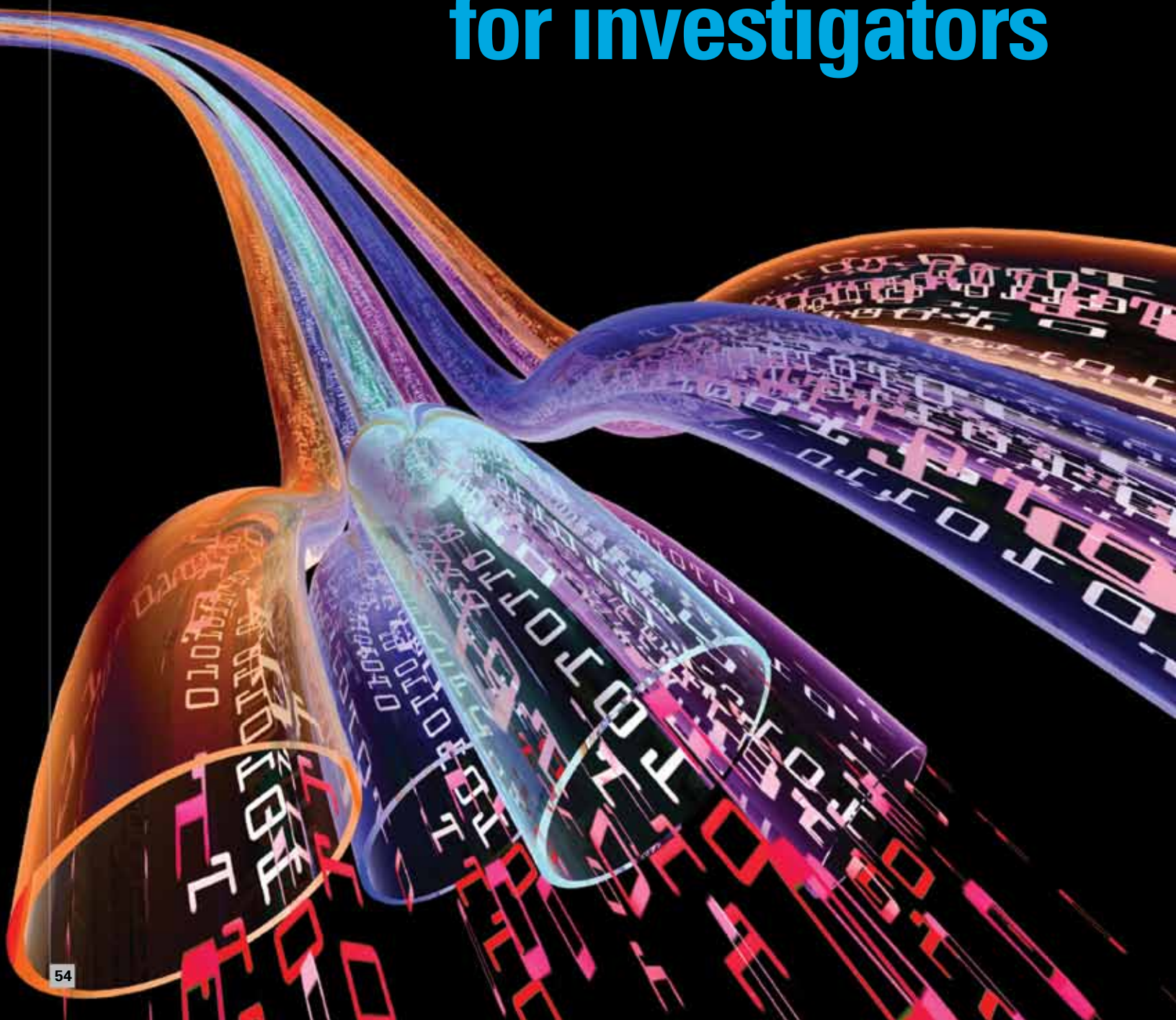
Within the conclusion and enterprise views, a heat map may serve as a compass allowing executive management to see in which direction they should be looking. Risk accurately assigned to those business units owning clients, delivery channels properly identified and support areas responsible for the product, service, client, or process they support clearly outlined allows for an effective and accurate risk analysis. In addition, it is imperative to re-state findings in a high level executive narrative summary concentrating on areas that need to be addressed. As a result, management can more effectively and efficiently manage the AML and CTF risk present within the financial institution.

Last, it is imperative to communicate the results of the AML risk assessment to management and business units involved and identified with applicable AML and CTF risk. This communication must be administered from a "Top-Down" approach.

*Anthony J. Tricaso, CAMS, senior BSA/AML and OFAC analyst, Key Bank Cleveland, Ohio U.S.A., [Anthony\\_j\\_tricaso@keybank.com](mailto:Anthony_j_tricaso@keybank.com)*



# Demystifying the wire transfer for investigators



Money laundering investigations will undoubtedly involve a review at some time of wire transfers (sometimes called “electronic funds transfers”). Wire transfers have been a common means of laundering money to offshore accounts in jurisdictions known for being bank secrecy havens.

A wire transfer is initiated with a request by a customer to direct the transfer of funds elsewhere, either domestically or internationally. The request, usually made through a bank or similar financial institution, gives instructions through a system of messages by telephone, email, fax or other electronic means of communication. Before the proceeds reach their final destination, the funds may go through several financial institutions and transit jurisdictions using correspondent bank accounts, serial wires, cover payments, shell companies and off shore jurisdictions. This feature has made wire transfers, at least in the past, attractive to money launderers by adding complexity in the layering, or second phase of the money laundering cycle. In some cases, unscrupulous financial institutions have facilitated the transfer of illegally obtained proceeds by helping criminals launder funds through complex transactions using corporate vehicles and establishing special private wealth account privileges.

While there have been efforts in recent years to encode information in the wire transfer message that may enable investigators to better track the source and destination of the funds, it is helpful for an investigator to understand more fully how wire transfers operate and what information is actually available.

A wire transfer comprises two components: (1) the instruction, which includes information on both the originator and the beneficiary institutions, and (2) the actual movement or funds transfer. Instructions may be sent in a number of ways, typically through a financial institution, through electronic communication networks, email, fax, telephone, telex or other various interbank payment systems. The method most used in the banking industry to communicate transfer instructions to each other is through the use of a special financial telecommunications system known as the Society for Worldwide Interbank Financial Telecommunications, otherwise known as “SWIFT.” It should be noted that SWIFT operates as a messaging service only — it does not hold or

manage accounts and does not itself engage in the actual transfer of funds. The actual transfer is accomplished through the use of correspondent bank relationships, which will be discussed below.

SWIFT may be used for domestic and international transfers; however, some jurisdictions have alternative interbank payment systems available. For instance, in the United States, there are at least two other interbank payment systems available: Clearing House Interbank Payments System (CHIPS) and Fedwire Funds Service (Fedwire). The primary difference between these two systems and that of SWIFT is that both CHIPS and Fedwire can be more involved in the actual transfer of the funds. In addition, direct bank-to-bank and other intermediary payment systems are used by banks to move customer funds between institutions.

The actual funds transfer takes place through what is called a “book transfer.” A book transfer is basically an accounting process that physically moves funds from one account to another. If both the originating customer and the beneficiary customer have an account at the same financial institution, then an internal book transfer can take place between the two customer accounts. When funds are transferred between two unrelated financial institutions, a book transfer occurs through a correspondent or intermediary bank employed to bridge the relationship.

In the United States, many banks maintain correspondent accounts for the purpose of processing and clearing wire transfer transactions with other institutions that are members of and have access to CHIPS or Fedwire. This enables them to carry out wire transfers on behalf of their customers, even if they are not member institutions themselves. Correspondent banking relationships are commonly found between domestic and foreign banks because they can facilitate business and provide services to clients in foreign jurisdictions without the expense and burden of a bank having to establish a foreign presence. These correspondent banking relationships can then consummate the transfer of funds which have been authorized through SWIFT or other systems. If two banks do not enjoy a direct correspondent banking relationship to each other, they may have relationships with other banks that do have such correspondent banking relationships and may use those other banks as third parties to effectuate the actual transfer of funds.

## Decoding the wire transfer instruction

Many financial institutions have tried to incorporate anti-money laundering features in their wire transfer procedures. In many jurisdictions now, banks and other financial institutions are required to obtain certain information about the customer and the amount, source and purpose of the funds being transferred, as well as information about the beneficiary. This information is generally required to be kept and available for investigation should the need arise. In addition, the bank or financial institution will maintain its own documentation, such as advice statements confirming a wire transfer and the debit and credit memos sent by banks to their originating or beneficiary customers. These documents may be useful in ascertaining account numbers and the identity of the originating and beneficiary customers. Where such documents are unavailable, the process of identifying and tracing funds will necessitate an understanding of how to read and interpret the various messaging systems used to affect wire transfers.

Payment systems such as CHIPS and Fedwire use a separate messaging format for wire transfer communications between member institutions. SWIFT has implemented a standardized messaging platform to be used by financial institutions globally. Within SWIFT messages, there are industry-wide protocols for messaging formats, special codes for differentiating between information and direction, and encryption to prevent security breaches during data transmission. To identify the different types of SWIFT messages, there are numbers assigned to each of them. For example, if a message is identified as “MT 103,” the “MT” prefix stands for “message type,” and the three-digit number that follows denotes a specific SWIFT message type (in this case, “103” means a single customer/credit transfer). Within a message type, specific field codes are used to demarcate important information. Field 50 is an important field to focus on since it includes information about the ordering customer’s name and address. Since it is an open field, it can often include additional customer identification information required by law or by an institution’s internal policies. This can be useful in identifying the particular person authorizing the transfer, in the case of a corporate entity or useful identifiers to distinguish a customer from those with similar names.



SWIFT bank identifier codes (BICs) are another source for practitioners because these provide the name of the financial institution, jurisdiction, location and/or branch. BICs are generally eight characters in length and consist of a bank code (unique to the financial institution), a country code (to identify the jurisdiction where the financial institution is located), and a location code (that provides a geographic distinction within a jurisdiction). Sometimes, an additional three characters are used for a branch code (to identify the physical branch of a financial institution).

The chart on the right presents an example of what a SWIFT message looks like and some common codes used therein.

### Further investigation

In many cases, the investigator will need to access banks records beyond the wire message itself.

Relevant records may be found at both the originating institution, as well as the beneficiary or receiving institution. If any intermediate or correspondent banks were used in the transfer, their records should be obtained as well. For documents from the originating institution, consider looking at the following:

- Funds transfer request form
- Wire transfer copy
- Advice statement or confirmation of wire transfer
- Debit memo to originating customer
- Customer's monthly account statement
- Internal log of outgoing wires (correspondent bank logs, payment and processing logs)
- Journal entry

For documents from the beneficiary or correspondent institution, the investigator may want to review:

- Funds transfer request form
- Wire transfer copy
- Credit memo to beneficiary customer (if deposited)
- Customer's monthly account statement
- Journal entry
- Cashier's check
- Interbank book transfer information that banks keep for the purpose of clearing transactions

In addition, depending on the circumstances of the investigation, it may be important to obtain additional supplementary documents where available, such as:


:20:	PAYREF XT78305
:32A:	091010EUR#1010000#
:50:	[CUSTOMER NAME AND ADDRESS]
:59:	[BENEFICIARY NAME AND ADDRESS]

#### Code Interpretation

20	Transaction reference number (coded number assigned by the originating institution to identify the transaction)
32A	Value date, currency code, and amount of the transaction
50	Ordering customer (party ordering the SWIFT transaction)
59	Beneficiary (party designated as the ultimate recipient of the funds)

#### In addition to the above codes, other codes may include

52D	Ordering bank (financial institution initiating the SWIFT)
53D	Sender's correspondent bank
54D	Receiver's correspondent bank
57D	The financial institution at which the ordering customer requests the beneficiary be paid
70	Details of payment
71A	Details of charges for the transaction
72	Instructions from the sending bank to the receiving bank

- *Underlying payment documents.* Invoices, shipping documents, receipts, consultant contracts and other documents associated with a transfer can reveal significant information about funds in question.
  - *Know Your Customer or "KYC" information.* At the transaction level, the bank may not have identified the ultimate beneficiary when funds exited the account. KYC information may also be helpful in this regard.
  - *Book transfers between personal and corporate accounts.* Such transfers may be useful in detecting a layering scheme.
  - *SWIFT private gateways and name variants used by the financial institution.* A review of the separate SWIFT gateways used only for private banking clients within the bank and its various branches may uncover a separate and potentially special permission transaction originating through these gateways. SWIFT name variants used by the financial institution may reveal transfers through different avenues. A bank may have different wire transfer departments, addresses or internal ways of identifying itself. To ensure that the gateways and name variants are listed in the order to produce bank records, practitioners should consider gathering this information through interviews with bank officials.
  - *Suspicious transaction reports (STRs).* Where available, STRs or intelligence reports may reveal valuable wire transfer information and originator details.
  - *Transaction patterns at specific institutions.* When reviewing information obtained from smaller banks, practitioners may look for patterns of very large transfers relative to the bank's size (for example, a book transfer that amounts to 80 percent of the total money transferred for a particular bank over the course of a month).
  - *Repaired, returned and resent wires.* Monitoring systems will create warnings or alert notices for messages containing errors (such as incomplete originator information). Such messages are then set aside and alerted for manual review. Such documents will often be maintained by the originating and beneficiary banks and may reveal patterns of activity by a target or bank. 
- Kenneth Barden, JD, CSAR, CAMS, Modernizing Financial Institutions Project, Washington, DC, U.S.A., kennethbarden@gmail.com*



Association of Certified  
Anti-Money Laundering  
Specialists®

**ACAMS®**

# YOUR AD HERE

Don't miss your opportunity to reach a readership  
of over 10,000 AML Professionals

▲  
TO ADVERTISE HERE

**CONTACT ANDREA WINTER:**  
1.786.871.3030 | [AWINTER@ACAMS.ORG](mailto:AWINTER@ACAMS.ORG)

# Foreign direct investments and money laundering trends



This article examines the relationship between Foreign Direct Investments (FDIs) and money laundering on a global scale. There has been debate about whether money laundering centers attract foreign investments for the purpose of concealing the illicit origins of funds or if there is a global trend of decreased foreign investments to money laundering jurisdictions with lax money laundering controls due to the reputational risks that the money

laundering centers pose. The examination of this issue will be based on the FDI literature *Money Laundering as Motives for FDIs* and on an analysis of nearly 60,000 FDI projects that took place globally from 2003 to 2008.

## Illicit money flows as motives for FDI

There are a few empirical studies in the FDI literature that focuses on the illicit money flows as a determinant of FDIs. One of the

most outstanding working papers on this topic in terms of its conclusions is *Illicit Money Flows as Motives for FDI* by Joseph C. Brada (Arizona State University), Zdenek Drabek (World Trade Organization) and M. Fabio Perez (Wilfrid Laurier University), which examines the role of FDI in facilitating money laundering and capital flight using transition economies' FDI outflows show the extent to which FDI is caused by these motives. Their finding is of high interest, as

Figure 1: Total number of inbound FDI projects by country.

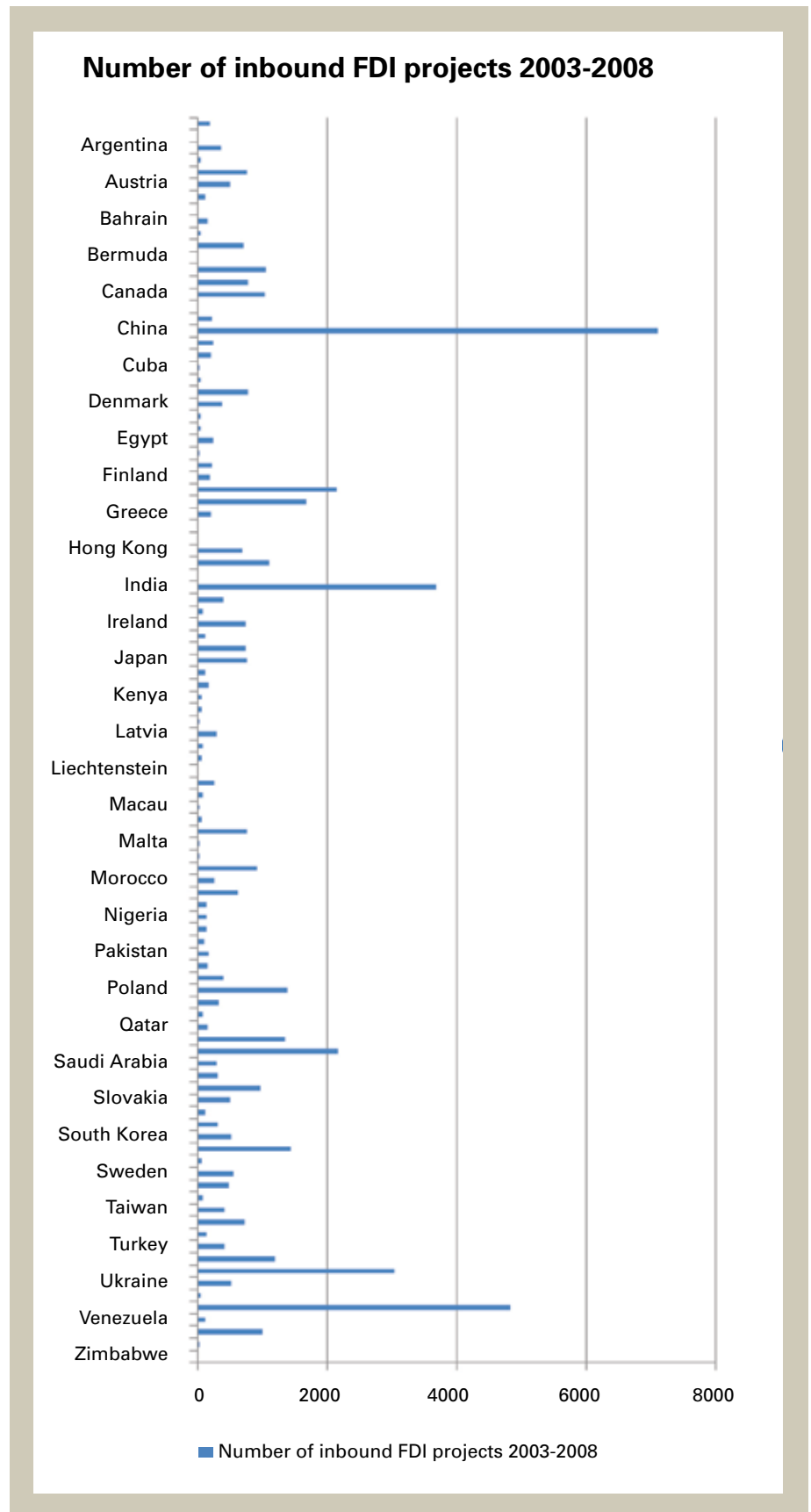
they suggest that illicit money flows influence both the choice of host countries for FDI and the volume of FDI outflows to these countries. Their paper estimates that 10 percent of total FDI flows and over half of FDI to money laundering countries are intended to facilitate illicit money flows.

**Money laundering stages, shell and front companies, trusts, nominees and other corporate vehicles**

Foreign investments by their nature can be used for money laundering purposes in various stages of the money laundering cycle. Compared to other commonly known money laundering methods, the amount of money involved in foreign investments is substantially high as these funds are being used to purchase factories, office buildings, machinery, construction materials and so on, depending on the industry giving the investment an air of legitimacy. This can be accomplished through the formation of shell and front companies in the placement stage that might commingle these funds with their revenue (if there is any) or use solely the illicit funds to invest in cross border jurisdictions with the purpose of concealing their true origin. To hide the ownerships, trusts, nominees and other corporate vehicles could be utilized which are among commonly known methods associated with money laundering. These investments can definitely be used at the integration stage of money laundering as well as through sales of these investments, whether they are in the form of business ventures or acquisitions of host country businesses. Tax evasion is also another significant facilitator of FDI decisions and transfer of funds to jurisdictions with lax money laundering controls and regulations.

**Utilization of correspondent banking**

In order to facilitate the transfer of these funds to host countries or money laundering centers, utilization of correspondent banking might be common as it is unlikely that money services businesses will be used to transfer such high amounts of funds since it will attract more suspicion. Rather, a large, well-known bank that has a correspondent banking relationship with a local respondent bank of the destination jurisdiction is more likely to be the choice of a money launderer.





## FDIs and reputational risk for the host country

The other side of the debate suggests that due to the reputational risks that jurisdictions with lax money laundering regulations and controls pose, there will be social and economic consequences including the slowing down of economic growth and development in these countries. Most financial institutions are likely to restrict transactions with businesses in these countries in order to mitigate their own risk as well as to comply with local and international AML and counter-terrorism financing (CTF) regulations. In this case, the launderers might not even have access to investing in these jurisdictions due to prohibitions or restrictions. Also, countries that have bad reputations or adverse publicity against them are likely to be risky for businesses to invest in.

## Global foreign direct investment patterns

In order to investigate which side of the debate is closer to reality, it is imperative to examine the global foreign direct investments projects that consist of the source and destination countries, global FDI projects as well as the total amount invested across borders.

## Data and analysis

The data was obtained from OCO Monitor, fDi Markets which is the most comprehensive database that provides the source company, source country, destination country, number of FDI projects, as well as jobs created. In total, from 2003 to 2008, nearly 60,000 FDI projects were recorded globally. The data also was used in the working paper: *Effects of Foreign Direct Investments by Multi-national Companies on Company Performance and on country Economic Growth* by Ayse Yuce (Ted Rogers School of Management) and Vefa Buyukalpelli (Global AML FIU, Royal Bank of Canada).

Table 1. TOTAL FDI (2003-2008)	
Total number of companies included in database	19,961
Total number of FDI projects (2003-2008)	58,204

The analysis includes a total of 58,204 foreign investment projects made by 19,961 companies from 103 countries between 2003 and 2008. Table 1 and Figure 1 illustrate the total number of inbound FDI projects between 2003 and 2008.

Figure 2: Total number of inbound FDI projects from 2003 to 2008

Country Name	Number of inbound FDI projects 2003-2008	Country Name	Number of inbound FDI projects 2003-2008	Country Name	Number of inbound FDI projects 2003-2008
Algeria	182	Guyana	9	Pakistan	168
Antigua	0	Hong Kong	685	Peru	157
Argentina	355	Hungary	1113	Philippines	396
Armenia	51	Iceland	14	Poland	1385
Australia	757	India	3679	Portugal	319
Austria	496	Indonesia	393	Puerto Rico	83
Azerbaijan	116	Iran	85	Qatar	156
Bahamas	7	Ireland	732	Romania	1346
Bahrain	156	Israel	115	Russia	2166
Bangladesh	49	Italy	735	Saudi Arabia	287
Belgium	701	Japan	761	Serbia & Montenegro	305
Bermuda	6	Jordan	108	Singapore	975
Brazil	1046	Kazakhstan	162	Slovakia	505
Bulgaria	778	Kenya	67	Slovenia	109
Canada	1042	Kuwait	70	South Africa	311
Cayman Islands	3	Kyrgyzstan	19	South Korea	523
Chile	226	Latvia	294	Spain	1428
China	7102	Lebanon	80	Sri Lanka	59
Colombia	243	Libya	70	Sweden	551
Croatia	196	Liechtenstein	2	Switzerland	478
Cuba	19	Lithuania	246	Syria	77
Cyprus	41	Luxembourg	71	Taiwan	415
Czech Republic	781	Macau	31	Thailand	719
Denmark	384	Macedonia	67	Tunisia	126
Dominican Republic	47	Malaysia	755	Turkey	416
Ecuador	43	Malta	36	UAE	1192
Egypt	237	Mauritius	26	UK	3040
El Salvador	29	Mexico	922	Ukraine	522
Estonia	226	Morocco	260	Uruguay	45
Finland	179	Netherlands	611	USA	4828
France	2144	New Zealand	135	Venezuela	117
Germany	1681	Nigeria	127	Vietnam	995
Greece	197	Norway	128	Yemen	22
Greenland	5	Oman	99	Zimbabwe	13

While interpreting these statistics, it is imperative to remember that there are various factors involved in investment decisions, and the purpose here is to demonstrate investment patterns into jurisdictions rated high risk in terms of money laundering as well as into those with lower risk rating. A close examination of Figure 2 demonstrates the low number of FDI projects in higher risk countries that have lax money laundering regulations and controls. For example, Antigua received no foreign investments from 2003 to 2008. Bahamas received 7, Cayman Islands received 3, Cuba 19, Dominican Republic 47, Ecuador 43, El Salvador 29, Guyana 9, Iran 85, Kenya 67, Krgyzstan 19, Liechtenstein 2, Zimbabwe 13, Yemen 22, Uruguay 45, Syria 77 and Sri Lanka 59.

Note that these numbers are quite low compared to inbound FDI projects in lower risk countries that have higher political stability and better international reputations.

**Conclusion and policy implications**

The overall examination of FDI trends and studies in the literature on the relationship between foreign investments and money laundering reveals that investing across borders in transition economies has been

used for the purpose of concealing the sources of illicit funds and facilitating the entry of these funds into the financial system but not necessarily to jurisdictions recognized as money laundering centers.

Governments, regulators and international regulations (for instance FATF typologies, Wolfsberg Group, Basel Committee, etc.) have countermeasures to detect and deter more commonly known money laundering methods. In the case of detecting and deterring money laundering through foreign investments, more enhanced scrutiny of these companies will be required to accomplish this goal. One of the most important due diligence requirements would be auditing the financial statements of companies whose choice of location does not make economical sense.

The major determinants of FDI's such as labor cost, the host country's political stability, cost of raw materials, profitability, competitors' decision, etc. are widely known and are factors of common sense. Any investment decision that is unusual in nature or has irrational motives may indicate the existence of money laundering. Therefore, companies from transition economies investing across borders should be subject to enhanced scrutiny especially if the investment decisions

do not make economical sense or there is evidence that the purpose of those investments is not to generate profits.

Among those, auditing of balance sheets, income statements, statement of retained earnings and statement of cash flows in line with International Accounting Standards are crucial. Verification of documentation and invoicing associated with purchases of fixed assets, prepaid expenses, real estate, insurance, employee payroll and utilities will be necessary to confirm that the company is investing for the purpose of profit generation. If the investment is in the form of acquisitions of foreign entities, associated documentation should be audited as well. Finally, another countermeasure for those companies investing in high risk jurisdictions includes enhanced scrutiny of ownership structure, shareholders and the board of directors to mitigate risks associated with these persons who are the ultimate controllers of the company, and who may possibly be politically exposed persons. **▲**

*Vefa Buyukalpelli, CAMS, MA (Finance), AML Investigations, Global AML FIU, Royal Bank of Canada, Toronto, ON, Canada, vefa.buyukalpelli@rbc.com*

Association of Certified  
Anti-Money Laundering  
Specialists®  
**ACAMS**®

www.ACAMS.org  
www.ACAMS.org/espanol

**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.



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](mailto:info@acams.org) Online: [www.acams.org](http://www.acams.org)

# Napoleon's legacy:

## How 19th century thinking skews AML in the 21st century

*Editor's note: This article is the first in a series that examines how banks can better assess geographical risk. Both at client take-on and in transaction monitoring, geography plays a key role in helping banks carry out their risk-based approach to AML compliance. The first article looks at how banks determine which countries to risk rate.*

In 1815, after nearly a quarter century of constant war, Napoleon was close to defeat and Europe lay shattered. Austria, France, Russia and the United Kingdom, the major powers at the time, met in the Austrian capital to reassemble a broken continent. The Congress of Vienna redrew the map of Europe — shuffling duchies and principalities between countries until it achieved a weak balance among competing interests. In the end, a political system emerged containing 39 sovereign states, and many more nobles seeking to upgrade their territories to full members of this new international club.

At first glance, a 19th century meeting of European power brokers would appear to have nothing do with the 21st century fight against money laundering. But how banks conceptualize a geographical risk is often held hostage to the thinking of this bygone era.

### What makes a country a country?

Everyone can agree that France is a country. Benin is too. But why? It is generally accepted in international relations that a country needs to have a defined territory, a population and a government exercising sole authority over both. Theories differ on the last criterion for “countryhood.” Because the Congress of Vienna balanced the competing interests of so many sovereign states, any new state could upset the delicate equilibrium and trigger another continent-engulfing war. Therefore, the only way to admit a new member to the club of countries was for existing members to recognize the newcomer as a coequal sovereign state.

To put it another way: a country was not a country until other countries said it was a country.

The members-only club mentality created in the Congress of Vienna served to keep Europe mostly peaceful for the next 100 years. But it leaves banks' risk-based approach vulnerable.

### Recognizing the problem

Geography, along with product, industry and delivery channel, is a primary AML risk metric banks use to evaluate clients and transactions. But geography is actually a proxy for a more important factor: legal situation. When a bank looks at the geographies involved in a transaction, it is really looking at the AML legal and regulatory regimes to which the parties involved are subject. Did the bank sending the transaction have to identify its client thoroughly before giving him an account? Is the correspondent bank in the transaction allowed to open accounts for shell banks? Is money laundering a crime in the country this client comes from? How about corruption?

Because the countries associated with a client or transaction are such important proxies, banks put a lot of effort into determining which jurisdictions are high risk and which are not. But in assembling geographical risk ratings, many unquestioningly adopt the Congress of Vienna approach — rating only those countries that existing countries think are countries.

This approach overlooks on-the-ground realities in several places. A good example is the Turkish Republic of Northern Cyprus (TRNC). Following a 1974 coup in the Republic of Cyprus, Turkey sent troops to protect the ethnically Turkish population inhabiting the northern third of the island. Under Turkish protection, the northern part of Cyprus would establish a separate state complete with president, prime minister, parliament and judiciary. Despite forming a semi-presidential representative democracy,



the TRNC is not recognized as a country by any country other than Turkey.

Because the TRNC is not a recognized country, most banks do not include it in their geographical risk assessments. This poses an anti-money laundering (AML) problem. Clients or transactions originating from Nicosia (the divided city that is capital to both the Republic of Cyprus and the Turkish Republic of Northern Cyprus) could be subject to two very different legal situations and thus represent distinct AML risks. The Republic of Cyprus is a member of the EU and signatory to agreements and treaties to inhibit money laundering. However, it cannot comply with any of its obligations in the TRNC territory. The TRNC, on the other hand, considers itself independent and unbound by the treaties and agreements made by the Republic of Cyprus. Because it is not recognized as a legitimate country, the TRNC cannot be made party to treaties and agreements inhibiting money laundering.

In effect, the northern third of Cyprus is an AML black hole: technically part of a country that has all the legal mechanisms to prevent money laundering, but no ability to enforce them and represented by a government unbound by treaties or agreements because no other country recognizes it as able to enter into them.

### Montevideo mitigations

Almost 120 years after the last delegate left Vienna, another conference on the other side of the world codified a more AML-friendly



definition of country. Under criteria laid out in the the Montevideo Convention, recognition from other countries was not needed. Beyond territory, population and government, a state only needed the capacity to enter into relations with other countries in order to be considered a country itself.

To put it another way: if it looks like a country and acts like a country, it is a country no matter what other countries have to say.


Using the Montevideo definition as a basis for geographical risk rating makes sense because it solves the limited-recognition problem. With a defined territory and popu-

lation, established government and ability to enter into relations with other countries, the TRNC would be included. So would several other limited-recognition countries dotting the world.

*See below for additional unrecognized and limited-recognition jurisdictions around the world.*

One of the challenges of international relations is that there is no supreme power to impose common definitions and approaches. Thus, the Declarative Theory of Montevideo exists today with the Constitutive Theory of Vienna — each country free to choose which

theory it wants to use when a new territory seeks to become a member of the club of countries. In reality, many countries select the more expedient theory to fit their policy and purposes.

Banks should do the same. 

*Max R. Tappeiner, Global AML advisor, Royal Bank of Scotland NV, Amsterdam, Netherlands. max.r.tappeiner@rbs.com*

*The views expressed in this article are those of its author and do not necessarily represent the views of the Royal Bank of Scotland Group.*

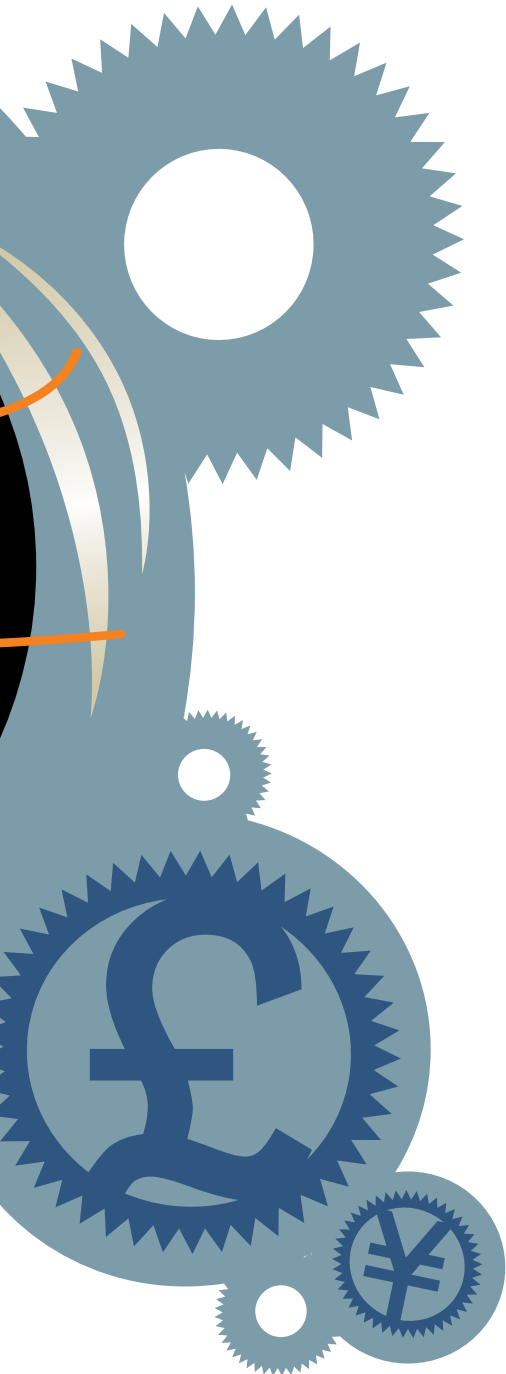
## Other AML Black Holes: Unrecognized and Limited Recognition Countries

The Turkish Republic of Northern Cyprus is one of several AML black holes scattered around the world. Officially termed “countries with limited recognition,” they are more likely to be referred to in the press as “break-away” or “disputed” territories. Regardless of the name, these areas represent the same AML risks: a central government nominally in control of territory but whose on-the-ground authority is contested by another government. In many cases, the un-recognized governments exercise legitimate powers like issuing passports and controlling territorial borders.

Country	Capital	Location	Recognition	History	Issues Passports	Exercises Territorial Sovereignty
Abkhazia	Suhkumi	Black Sea / Caucasus	Russia, Nicaragua, Venezuela, Nauru	Declared independence from Georgia in 1992	Yes	Yes
Kosovo	Pristina	Southeast Europe	71 of 191 UN member-states, including most, but not all, members of the EU	Declared independence from Serbia in 2008	Yes	Yes
Nagorno-Karabakh	Stepanakert	Caucasus	No UN member-states recognize Nagorno-Karabakh	Declared independence from the Soviet Union in 1992. Territory claimed by Azerbaijan	No	Yes
Palestine	Jerusalem	Eastern Mediterranean	Due to the ambiguous nature of statements around the issue of Palestinian statehood, it is estimated that between 115 and 130 countries recognize Palestine	The Palestine Liberation Organization declared Palestinian statehood in 1988 from Algiers	Yes	No
Sahrawi Arab Dem. Rep.	El Aaiún	Northwest Africa	57 countries recognize the SADR and 8 other recognize but have “frozen” or otherwise suspended recognition pending a referendum of self-determination	With the end of Spanish colonial rule, neighboring countries sought to annex the Western Sahara territory. A local political movement declared independence in 1976. Morocco occupies most of the claimed territory of the SADR	Yes	Partial
Somaliland	Hargeisa	Horn of Africa	Not officially recognized by any country, however, several countries have non-diplomatic political relations with Somaliland	Declared independence from Somalia in 1991 following the collapse of the Somali government during the Somali Civil War	Yes	Yes
South Ossetia	Tskhinvali	Caucasus	Russia, Nicaragua, Venezuela, Nauru	Declared independence from Georgia in 1991	Yes	Yes
Transnistria (Trans-Dniestr)	Tiraspol	Black Sea	Not officially recognized by any country	Declared independence from Moldova in 1990	Yes	Yes
Turkish Rep. of N. Cyprus	Nicosia	Eastern Mediterranean	Turkey	Following a 1974 coup, the TRNC was established by ethnic Turks occupying the northern part of Cyprus	Yes	Yes



# Combating trade-based money laundering through global partnerships



Homeland Security Investigations (HSI), the investigative arm of U.S. Immigration and Customs Enforcement, has been a leader in the pursuit of trade-based money laundering investigations. Due to its unique authority and access to both trade and financial data, HSI is strategically positioned to combat criminal organizations exploiting vulnerabilities in the global trade and financial systems.

## What is trade-based money laundering?

Trade-Based Money Laundering (TBML) is a type of money laundering where criminals use the international trade system to disguise illicit proceeds by altering customs and banking paperwork, making it appear as legitimate. Unfortunately, vulnerabilities in the international trade system provide numerous opportunities for exploitation. Some criminals simply depend on the sheer volume of international trade to hide their crimes. Others rely upon the complexity of foreign exchange transactions and diverse financing instruments to conceal their fraudulent activity. Many traditional customs fraud methods such as false-invoicing, over-invoicing and under-invoicing commodities are often used to move value around the world. To further increase the value of their illicit funds, criminals often layer various schemes.

## Black Market Peso Exchange

One well-known example of TBML, used extensively by Colombian drug cartels to repatriate drug proceeds, is commonly referred to as the Black Market Peso Exchange (BMPE). BMPE operates as an underground financial exchange system used to evade record keeping requirements mandated by the Bank Secrecy Act (BSA) in the U.S., as well as to evade Colombian bank

reporting requirements, customs duties, sales tax and income tax. The overall scheme involves the purchase of U.S. export goods destined for Colombia with proceeds from the sales of illegal drugs.

The following scenario demonstrates how a Colombian cartel could use BMPE to launder illicit funds. A Colombian cartel sells cocaine in the U.S. and receives illicit U.S. dollars. The cartel then contacts a Colombian peso broker to launder their money. The peso broker arranges to have the illicit proceeds picked up from the cartel and placed into U.S. financial institutions, often by structuring deposits into various bank accounts. Next, the peso broker finds Colombian importers who want to import U.S. goods, and U.S. exporters who will export goods to Colombia.

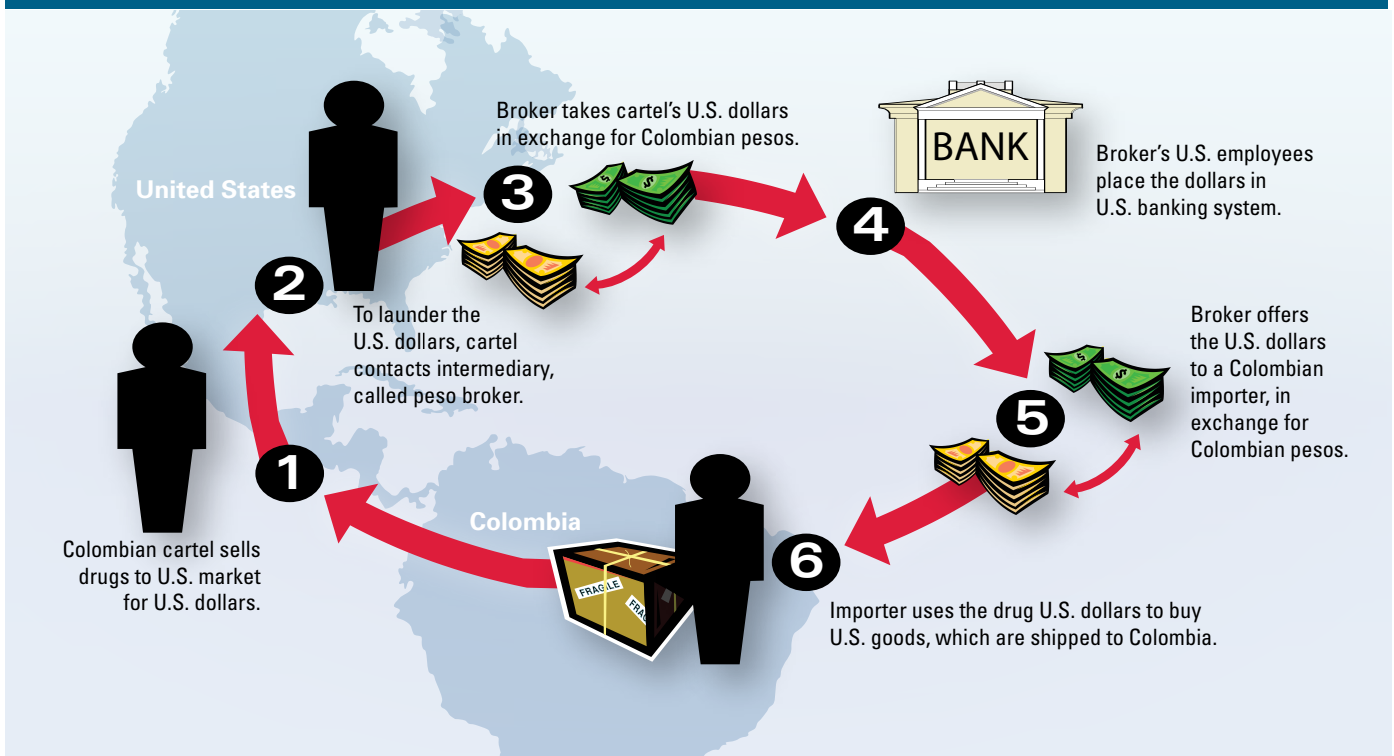
Once these relationships are established, the peso broker uses the illicit proceeds already embedded in the U.S. banking systems to pay the U.S. exporters for the shipments to Colombia. Therefore, the illicit proceeds never leave the U.S. The peso broker then directs the exporter to ship his goods to a specified Colombian importer. The Colombian importer receives the goods and then pays the Colombian peso broker in pesos for the shipment. The peso broker then returns the clean pesos to the drug cartel. All of the participants benefit from the transaction by either increasing their sales and/or charging a fee for their participation. In addition, the Colombian importer can easily falsify its invoices reducing or avoiding Colombian customs duties.

## Trade Transparency Units

When it comes to TBML, one of the primary factors criminals rely on besides the complexity of the international trade transaction is the idea that a customs agency can



Example of Money Laundering through Global Trade



Source: U.S. Immigration and Customs Enforcement

only see one side of a trade transaction. For example, if a U.S. exporter sends \$1 million dollars worth of computers to Brazil, U.S. customs officers do not know what is being reported upon entry to Brazil. A Brazilian importer in collusion with the exporter could easily change the paperwork to reflect the value of the shipment as \$500,000. This would allow the Brazilian importer to justify a reduced payment of \$500,000 to the U.S. exporter, transferring \$500,000 additional dollars in value to Brazil.

This example is a typical TBML scheme called undervaluing. By invoicing the goods below the fair market value, the exporter can transfer value to the importer. Once the importer sells the goods, he will receive the full value of merchandise. In this example, since the importer only paid \$500,000 to the exporter, he still owes the exporter \$500,000 because the true value of the shipment was \$1 million. This portion of the debt can be settled using a parallel banking market like the BMPE or a similar Brazilian Black Market scheme called *Dolerios*. However, if both the U.S. and Brazilian customs agencies could

see each other's trade paperwork, the transaction becomes transparent, allowing law enforcement personnel to identify fraudulent transactions indicative of money laundering and other crimes.

This transparency is the theory behind the initiation of HSI's Trade Transparency Unit (TTU) initiative. The TTU is a collaborative effort among HSI, U.S. Customs and Border Protection (CBP), the Department of State and Department of the Treasury. The first TTU was established in Washington D.C. at HSI headquarters. At that time, HSI began identifying countries who were interested in partnering and sharing trade data. Currently, HSI has developed partnerships with Argentina, Brazil, Colombia, Mexico, Panama and Paraguay. Through these relationships, HSI and foreign TTUs exchange trade data, allowing visibility to both sides of a trade transaction.

HSI TTUs bring worldwide recognition to the threat of trade-based money laundering and HSI's efforts to combat and prevent this threat. Recognized as the best mechanism

to combat trade based money laundering, TTUs have been highlighted in numerous U.S. government publications including *The National Money Laundering Threat Assessment*, the *Department of Treasury's National Money Laundering Strategies* and the *Department of State's International Narcotics Control Strategies*.

Using specialized software and proven investigative techniques, officers can analyze trade and financial data to help identify trade transactions and other information that does not follow normal patterns. To help conduct this analysis, HSI has developed a specialized computer system called the Data Analysis & Research for Trade Transparency System (DARTTS). This program is used by both HSI and foreign TTU partners to help identify indicators of money laundering, customs fraud, contraband smuggling and the evasion of duties and taxes.

By establishing these international partnerships, TTUs offer another means to link global customs and law enforcement agencies together, expanding networks to help

combat transnational crime. Over the past several years, these joint efforts have identified and disrupted the activities of criminal organizations engaged in fraudulent trade schemes, BMPE, money laundering, and illegal exportation of goods, resulting in multiple arrests and seizures of millions of dollars of proceeds and merchandise.

### Recent investigative successes

HSI, as part of the Joint Terrorism Task Force, initiated a case to investigate the suspicious exportation of electronic goods from Miami, Florida, to Ciudad del Este in Paraguay. Ciudad del Este borders Argentina and Brazil, and is part of a region often referred to as the Tri-Border Area. One of the largest duty-free zones in the world, Ciudad del Este is also a South American smuggling hotspot for counterfeit goods, illegal weapons and other illicit activities. In December 2006, Galeria Page, one of the large shopping centers within Ciudad del Este, was designated as a Specially Designated Global Terrorist (SDGT) entity by the Office of Foreign Assets Control, due to its ties to the terrorist group Hezbollah. Once an individual or business is designated as an SDGT, U.S. entities are prohibited from conducting business with the SDGT or face criminal prosecution.

The use of trade as an instrument to launder illicit revenue is a complex and evolving scheme which will challenge law enforcement for decades

As the investigation progressed, HSI special agents and CBP officers, along with JTTF taskforce members, determined several Miami based freight forwarding companies were illegally exporting electronic goods to Galeria Page. Working with TTU partners in Paraguay to verify paperwork, agents discovered the criminals concealed the true destination of the prohibited shipments by using fake invoices containing false addresses and fictitious ultimate consignees on required export paperwork. In addition, wire transfer

### Red flag indicators of trade-based money laundering

-  Payments to a vendor made by unrelated third parties
-  Payments to a vendor made via wire transfers from unrelated third parties
-  Payments to a vendor made via checks, bank drafts, postal money orders or travelers checks from unrelated third parties
-  Suspected or known use of shell companies and related accounts
-  Unexplained, repetitive or unusual patterns of wire activity
-  False reporting: such as commodity misclassification, commodity over-valuation or under-valuation
-  Carousel transactions: the repeated importation and exportation of the same high-value commodity
-  Commodities being traded not matching businesses involved
-  Unusual shipping routes or transshipment points not making economic sense
-  Packaging inconsistent with commodity or shipping method
-  Double-invoicing
-  Discrepancies between invoiced value of the commodity and the fair market value
-  Payment for the goods either in excess or below known market value
-  Size of the shipment inconsistent with the average volume of business

payments were routed through various facilities to mask their true origin.


As a result of the investigation, four individuals and three Miami based freight forwarding companies were indicted on conspiracy charges for violating the International Emergency Economic Powers Act (IEEPA) and the smuggling of electronic goods. As of October 2010, three of the four have pled guilty. In addition, more than \$119 million dollars of merchandise, primarily high-end electronics, have been seized as part of the investigation.

A second large scale TBML investigation involved a BMPE scheme operating out of a Los Angeles based toy company. Drug proceeds, which were allegedly laundered through structured cash deposits, were used to purchase stuffed animals, including teddy bears. The toys were subsequently exported to Colombia for sale and the Colombian pesos generated by those sales were then used to reimburse the Colombian drug traffickers.

In July 2010, defendants associated with the toy company and money laundering organi-

zation were indicted under charges including structuring transactions to avoid reporting requirements, bulk cash smuggling and intimidation of witnesses. In addition, the toy company as a whole was charged with conspiracy to launder money. Based on the criminal indictments for structuring, a criminal forfeiture indictment of \$8.6 million for structured assets was also filed.

The use of trade as an instrument to launder illicit revenue is a complex and evolving scheme which will challenge law enforcement for decades. But with the development of the HSI TTU and its global partners, as well as the continuing commitment by HSI demonstrated by the steady expansion of the program, law enforcement can effectively combat the ever-changing world of TBML.

For additional information on the TTU or TBML, please contact the TTU Unit Chief at [TTU.TTU@dhs.gov](mailto:TTU.TTU@dhs.gov). 

*Jennifer Eisner, section chief, Trade Transparency Unit, Homeland Security Investigations, Washington, D.C., U.S.A. [Jennifer.Eisner@dhs.gov](mailto:Eisner@dhs.gov)*

# The Foreign Account Tax Compliance Act: Stay tuned to see its effects

The U.S. has had a long history of trying to stop tax evasion by its citizens and residents who use foreign accounts with only limited success. A highly sophisticated offshore industry, comprised of financial professionals, bankers, brokers, corporate service providers, tax attorneys, accountants and trust administrators, advise and assist Americans on opening offshore accounts and concealing assets in order to avoid taxes and creditors in their home jurisdictions.<sup>1</sup>

Congress has estimated that every year the U.S. loses nearly \$100 billion in tax revenues due to offshore tax abuses.<sup>2</sup> On March 18, 2010, Congress passed broad-sweeping legislation called the Foreign Account Tax Compliance Act (FATCA) in an effort to combat offshore tax dodging by “U.S. persons,” including U.S. citizens or residents of the U.S., privately held corporations, partnerships and estates. While most of its effects do not take place until after December 31, 2012, FATCA has such an onerous effect on foreign financial institutions (FFIs) that choose to do business with “U.S. persons” that these institutions need to start preparing for it as soon as possible.

In general, it creates a complex withholding regime designed to penalize FFIs and foreign entities that refuse to divulge the identities of their U.S. clients. While there have been many investigations into offshore tax abuses, the Act comes on the heels of two large recent tax scandals, one involving the LGT Bank in Liechtenstein and one involving UBS in Switzerland. It also comes at a time when the U.S. has given large subsidies to the banking sector and when the country, due to a huge deficit, is badly in need of more tax revenue. This article will provide some background on the existing legislation, briefly describe FATCA, raise some outstanding questions and concerns and set forth some

steps that foreign FFIs can take immediately to ensure they are prepared to comply with the Act by 2013.

## Background on stopping tax evasion

In 2001, the U.S. government established the Qualified Intermediary Program (QIP), the existing legislation dealing with tax evasion. It encouraged (but did not require) FFIs, known in the legislation as Qualified Intermediaries (QIs), to sign an agreement with the IRS to act as U.S. withholding agents and comply with the withholding obligations set out in U.S. tax law for their U.S. clients. Each QI is required to decipher the nature and amount of their customers’ U.S. source income, determine whether customers are eligible for treaty benefits based on the clients’ national residency and then calculate and report the proper amounts to the IRS. The QIP also requires them to have know-your-customer procedures (KYC) in place to verify and document the beneficial owner of each of its accounts, and each QI must utilize external auditors to ensure compliance. However, as part of this agreement, the QIs are not required to disclose the identities or nationalities of their clients. The QIs were strongly opposed to doing so, not only because it opened the door for competition from U.S. financial institutions, but also because it undermined their bank secrecy policies.<sup>3</sup>

The QIP has had its share of flaws. First, the QIP is voluntary so there are many FFIs that do not participate in the program. Because of this, there is a great amount of under withholding and improper granting of tax exemptions and tax treaty benefits. Secondly, the ability of U.S. persons to establish offshore corporations, trusts and foundations (sometimes encouraged by QIs) allows some U.S. taxpayers to inappropriately receive exemp-

tions or evade taxes altogether simply because they hold their funds in these vehicles. The current KYC rules, for the most part, do not require FFIs to obtain information on the beneficial owners of these entities. In addition, in many situations involving QIs there has been no investigation of fraud or illegal acts.<sup>4</sup>

It is not just the U.S. that is trying to stop tax evasion. There have been several multinational organizations like the Organization for Economic Cooperation and Development (OECD) and the European Union Savings Directive that have tried to stop tax evasion internationally and promote tax information exchanges. The OECD has been able to reduce the list of “uncooperative tax havens” considerably over the last decade. However, there are still countries that have significant restrictions on disclosing bank information. Many of these countries enact laws that allow nonresidents to form companies, trusts, foundations and other legal entities at low costs and hold their assets in financial accounts protected by secrecy laws that are enforced with criminal and civil penalties.<sup>5</sup>

In its latest publication, the Global Forum on Transparency & Exchange of Information for Tax Purposes stated:

*“More and more frequently, people today work in more than one jurisdiction, multinational corporations organise their affairs in increasingly complex webs of subsidiaries and holding companies, foreign bank accounts can be set up in a matter of minutes on the web, and trusts can be established to manage family wealth for children and grandchildren in dozens of different jurisdictions. It is no longer possible for any jurisdiction to rely only on information available within its own borders to enforce its own laws.”<sup>6</sup>*

<sup>1</sup>U.S. Senate Permanent Subcommittee on Investigations, Tax Haven Abuses: The Enablers, The Tools and Secrecy, (August 1, 2006): 1.

<sup>2</sup>Senator Levin, Senate Congressional Record, S1745: Hire Act, March 18, 2010.

<sup>3</sup>U.S. Senate Permanent Subcommittee on Investigations, Tax Haven Banks and U.S. Tax Compliance, July 17, 2008, 21-26.

<sup>4</sup>U.S. Government Accountability Office, Qualified Intermediary Program Provides Some Assurance That Taxes on Foreign Investors Are Withheld and Reported, but Can Be Improved, December 2007.

<sup>5</sup>Id at 26-36.

<sup>6</sup>OECD (2010), Tax Co-operation 2010: Towards a Level Playing Field, OECD Publishing, <http://dx.doi.org/10.1787/taxcoop-2010-en>.





### A brief description of FATCA

The following is a brief summary of FATCA but by no means is meant to include all details and provisions. FATCA significantly extends and broadens reporting requirements for certain foreign entities regarding “U.S. persons.” Foreign entities can no longer conceal the identity of their U.S. customers as they were able to in the QIP. The U.S. will rely on FFI and non-financial foreign entities (NFFE) that have U.S. clients to provide information about their identity in order to assist them in trying to stop U.S. tax evasion. If they do not, they must terminate their relationships with their U.S. clients or choose to pay a 30 percent withholding

penalty on “withholdable payments.”<sup>7</sup> “Withholdable payments” for the purposes of this Act, include U.S. source FDAP income (e.g., interest, dividends, etc.) and gross proceeds from the sale of property which can produce interest or dividends from U.S. sources.<sup>8</sup>

The definition of FFIs has been broadened to include not just banks but institutions such as brokerage firms, investment companies and hedge funds, as well as their affiliates. FFIs can elect to be treated as U.S. financial institutions and file IRS Form 1099 for each U.S. account holder or they have the option of entering into an agreement with the IRS to put procedures in place which identify U.S. account holders. This requires annu-

ally reporting the name, address, tax identification number (TIN), account number, account balance, gross receipts and gross withdrawals for each account.<sup>9</sup> The FFI must also withhold 30 percent of any “pass thru payments” made to recalcitrant account holders who do not wish to comply with the disclosure.<sup>10</sup> Where a foreign law would prevent the reporting of information, the FFI would attempt to obtain a valid and effective waiver of such law from account holders. If such waiver is not obtained, then the account would be required to be closed. Non-participating FFIs, who do not sign the agreement, face the 30 percent withholding tax on all “withholdable payments.”<sup>11</sup>

In preliminary guidance from the IRS, Notice 2010-60, certain FFIs have been excluded from complying with FATCA. Among the exclusions are insurance companies that issue insurance with no cash value (e.g., property and casualty and term life insurance); start-up companies for the first 24 months of commencing business; and retirement plans sponsored by a non-U.S. employer with no U.S. participants or beneficiaries.<sup>12</sup>

A NFFE is defined as any other entity that does not fall under the definition of an FFI including privately held operating businesses, professional services firms, foreign trusts and foreign partnerships.<sup>13</sup> In order for an NFFE to avoid the 30 percent withholding tax, they must either be exempt from taxation; be a publicly traded company (or an affiliate of a publicly traded company); certify that they have no substantial U.S. owners (those that directly or indirectly own greater than 10 percent of the entity); or they must disclose the name, address and TIN of each substantial U.S. owner to a withholding agent or the IRS.<sup>14</sup>

There are also new reporting requirements for any individual who has an interest in a foreign asset and penalties for those who do not comply. These requirements are supplemental to the current FBAR requirements.<sup>15</sup>

In addition, a *de minimis* exemption is provided for all U.S. account holders with

<sup>7</sup>Code Sec. 1471(a).

<sup>8</sup>Code Sec. 1473(1)(A)(i). Any payment of interest (including any original issue discount), dividends, rents, salaries, wages, premiums, annuities, compensations, remunerations, emoluments and other fixed or determinable annual or periodical gains, profits and income, if such payment is from sources within the U.S.

<sup>9</sup>Code Sec. 1471(c).

<sup>10</sup>Code Sec. 1471(b)(1)(D). Includes any payment that is attributable to a withholdable payment.

<sup>11</sup>Code Sec.1471(b)(1)(F).

<sup>12</sup>IRS Notice 2010-60.

<sup>13</sup>Code Sec.1472(d).

<sup>14</sup>Code Sec.1472.

<sup>15</sup>Kevin E. Packman, Esq. and Mauricio D. Rivero, Esq., “The Foreign Account Tax Compliance Act Taxpayers Face More Disclosures and Potential Penalties,” *Journal of Accountancy* (August 2010): 1. Report of Foreign Bank and Financial Accounts which must be filed by U.S. persons having a financial interest in or signature authority or other authority over any financial account in a foreign country if the aggregate value of these accounts exceeds \$10,000 at any time during the calendar year.

depository accounts less than \$50,000.<sup>16</sup> The IRS has stated that FATCA will require electronic reporting and they will be creating new forms and agreements.<sup>17</sup> Unresolved questions still remain and there will be further workable implementation guidelines from the Treasury Department to come.

### Questions and concerns

FATCA definitely makes it more difficult for “U.S. persons” to hide assets in offshore accounts. No doubt, it is a big step forward in creating a more transparent and accountable global financial world. It may also set a standard for the rest of the world to adopt in order to avoid tax evasion in their countries.

But there are many questions that arise. First, is such an Act that is so highly burdensome to both the IRS and the international financial community worth the cost?

According to the Joint Committee on Taxation, FATCA is only estimated to recover \$8.7 billion in U.S. taxes over the next 10 years.<sup>18</sup> This is a far cry from the \$100 billion estimated by Congress to be lost on an annual basis due to tax evasion. Why is there such a difference? Is this an overestimate by Congress; an underestimate by the Joint Committee on Taxation, or is FATCA only going to stop a small portion of U.S. tax evasion?

Undoubtedly, the costs of implementing FATCA are going to be staggering for FFIs. The inherent risks, complexities of building extensive technology systems and legal challenges, especially in instances where FATCA conflicts with an FFIs’ domestic laws, provide an enormous burden for FFIs. The European Banking Federation and the Institute of International Bankers, in their public comment to the IRS, stated that many large institutions have conservatively estimated that it will cost, on average, about \$10 to review each account and properly identify whether it is an account beneficially owned by a “U.S. person” or not. Many of these institutions have between 30-50 million accounts.<sup>19</sup> There is concern in the interna-

tional community that FATCA is a one-size-fits-all solution which is too all encompassing for FFIs, some of which have very few U.S. customers. Some argue that FATCA should be more risk-based, reducing documentation, reporting and withholding requirements for those entities, accounts and payments that are low-risk.

Although it will be costly, most of the larger institutions will comply with FATCA because they have enough resources to afford legal, accounting and the technological assistance to implement the Act. It is the smaller institutions that might suffer due to high costs and lack of personnel with knowledge of the U.S. tax laws. It is even difficult for many U.S. attorneys to try to unravel and comprehend the U.S. Internal Revenue Code. So how can we expect a small institution in a foreign country whose employees do not speak English to be able to understand and have the wherewithal to comply with U.S. tax laws? Will FATCA cause takeovers of smaller financial institutions that have to divest themselves of U.S. customers or withdraw from investing in the U.S. markets?


The original version of FATCA included provisions to impose reporting requirements on “material advisors,” including attorneys and accountants who earn more than \$100,000 per year assisting in the direct or indirect creation or acquisition of an interest in a foreign entity.<sup>20</sup> This provision was not included in the final version of the Act. So, not only were they left out of the Act, but it is clear that these professional service providers will greatly benefit from FATCA as they will be needed to assist FFIs and NFFEs around the globe in understanding and complying with the provisions of the Act. Is it possible that their omission from the Act could come back to haunt the U.S.?

American citizens living abroad are undoubtedly afraid not just of the costs that could be passed down to them by FFIs but also of the risk that their financial accounts could be closed. Some FFIs might not be able to afford to deal with the compliance required to keep them as clients. Discrimination against

Americans living abroad might also occur as a consequence of the Act. According to the American Citizens’ Abroad Comments on FATCA,

*“U.S. citizens residing abroad are standing in the middle of this crossfire and they are the clear losers — unable to maintain banking relationships in the United States, unable to procure banking relationships overseas but still needing banking services to pay U.S. taxes, invest funds and simply to live in a modern economy.”*<sup>21</sup>

### Steps to take right now

Although the Treasury has not yet issued final guidelines, there are steps that FFIs should be taking immediately. First of all, the Treasury is asking the public for their comments on FATCA, so if an FFI or organization has comments, now is the time to send them to the Treasury Department.<sup>22</sup> In addition, each FFI should create an internal FATCA task force in order to develop a clear understanding of the Act and assess the current situation with respect to accounts held by “U.S. persons.” Included in the task force should be legal, tax, AML and technology personnel. This task force needs to identify all parties affected by the Act and educate their employees about FATCA, especially their compliance personnel and relationship managers or anyone who interacts with the public. It should be determined how many U.S. clients the FFI has and what information is already in its database regarding the identity of its U.S. clients. Then the task force should put together a to-do list for its application developer so that there will be an electronic database in place by 2013. Each FFI should also determine the best way to make its U.S. customers aware of FATCA. If each organization waits for the final regulations from the Treasury Department, it could be too late to ensure compliance by 2013. 

*Diane Eisinger, J.D., LL.M.; CFP®, CAMS, vice president, Spectrum Advisors, Inc. Williamsburg, VA, U.S.A., Diane6022@gmail.com*

<sup>16</sup>Code Sec.1471(d)(1)(B).

<sup>17</sup>IRS Notice 2010-60.

<sup>18</sup>Joint Committee on Taxation Report, JCX-5-10, February 23, 2010.

<sup>19</sup>European Banking Federation and the Institute of International Bankers, Comments on Notice 2010-6- Providing Preliminary Guidance on FATCA, November 12, 2010, at 3.

<sup>20</sup>Dirk, J.J. Suringa, Esq., U.S. Withholding and Reporting Requirements for Payments of U.S. Source Income to Foreign Persons, January 19, 2010.

<sup>21</sup>American Citizens Abroad, Comments on Foreign Account Tax Compliance Act (FATCA) Provisions Incorporated in the Hiring Incentives to Restore Employment Act (HIRE, June 14, 2010).

<sup>22</sup>IRS Notice 2010-60





**Complying with Patriot Act anti-terrorist financing requirements.**

**Confronting cybersecurity challenges.**

**Capturing actionable intelligence.**

**Ready for what's next.** Complex money trails are hard to follow across global borders. Today's financial institutions must be adept at identifying individuals and networks that threaten national and world security. Booz Allen's experience in national security and banking offers a proven process and methodology to detect patterns of terrorist financing with certainty. Using a bank's existing anti-money laundering data, we can increase suspicious activity report filings to ensure compliance with terrorist financing laws. Whether you're managing today's issues or looking beyond the horizon, count on us to help you be ready for what's next.

Ready for what's next. [www.boozallen.com/fas](http://www.boozallen.com/fas)

**Booz | Allen | Hamilton**  
strategy and technology consultants





# Australasian Chapter

In November 2010, the Australasian Chapter undertook a modified nomination and election process for a new executive board at the Annual General Meeting (AGM). The nomination and election process is a requirement under the Chapter Handbook which gives all the chapter members a say in the composition of the new executive board and the option to join the board themselves. This certainly was the case with the Australasian Chapter. Although the AGM itself was held the 23rd of November the nomination and election process took place throughout November. ACAMS' head office provided support to the chapter with the undertaking and marketing of the nomination process.

The results of the election showed that there is an ever increasing interest in not only the workings of the board but the chapter in general. The make up of the new 15 person executive board is: Guy Boyd (co-chair); Aub Chapman (co-chair); Erum Khan (co-secretary); Gavin Coles (co-secretary); Julie Beesley (co-treasurer); Stuart Hansen (co-treasurer and co-programming, New Zealand); Tim Land (co-membership); Phil O'Connell (co-membership); Paddy Oliver (co-communications); Crispin Yuen (co-communications); Bill Brown (co-programming, Melbourne); Graham Gorrie (co-programming, Sydney); Alex Tan (co-programming, New Zealand); Dr. Hugh McDermott (co-programming, webinars); Brett Webber (co-programming, webinars). The New Zealand-based board members, Stuart, Phil and Alex, are supported by New Zealand Working Group members, Gary Hughes and Tim Morrison. By expanding the numbers on the board, together with more focused board portfolios, the executive board aims to provide more targeted activities for chapter members.

The AGM was held at the KPMG office in Sydney with a video link to Melbourne. Attendees heard from Lindsay Chan of the Asia/Pacific Group on Money Laundering (APG secretariat), followed by Aub Chapman (co-chair) who, on behalf of the outgoing board, reported on the chapter's first three years.

Lindsay gave a comprehensive overview of APG's thoughts on emerging AML issues for



Pictured from L to R: Board Director, Alex Tan; Guest presenters in Auckland from OFCANZ, Malcolm Burgess and Brett Kane; Group member, Gary Hughes

the Asia Pacific region for the next two to three years. After an overview of the membership of APG, Lindsay concentrated on several themes. First, the money laundering issues of concern in the region which include: corruption, fraud, tax havens, illegal logging and human trafficking. Regional weaknesses was the second theme. Lindsay touched on gaps in legal frameworks, lack of awareness of FATF standards and a lack of resources. The final theme related to FATF's ongoing review of the 40+9 Recommendations. This topic sparked a lively discussion, particularly on the R.5 topic of beneficial ownership.

Aub's report touched on the history of our chapter since its formation in 2007. Touching upon the board members themselves, Aub thanked all the past and present board members for their contributions. A brief summary of the members' activities that have taken place over the past three years was given with Aub thanking all the guest speakers and sponsors. Finally, Aub spoke about the future of the chapter and its direction in the Australasian region.


A copy of Lindsay's presentation and Aub's report can be found on the chapter webpage.

The board would like to thank the partners of KMPG for providing the facilities and excellent hospitality.

In New Zealand, ACAMS ran two very informative sessions in both Auckland and Wellington during November. Between 60 and 45 industry members attended each respective session. A presentation was given

by the director and operations manager of the Organised & Financial Crime Agency of NZ (OFCANZ). The presentation gave an insight into this new enforcement agency, their work, how they fit into the NZ enforcement environment and some case studies around AML. The case studies highlighted risks in NZ posed by company formation agents and money service bureaus. Representatives of New Zealand's three AML supervisors attended the sessions. The board would like to thank the partners of PWC for providing the facilities and excellent hospitality.

Moving forward the chapter will aim to increase its membership, liaise with industry and regulators, with the aim of being the leading AML/CTF professional organisation in the region.

The University of New South Wales (UNSW) is an official ACAMS partner and the Faculty of Law will in 2011 again be offering a course entitled "Anti-Money Laundering and Proceeds of Crime: Laws and Counter Measures." Students who successfully complete this course and become (or are) members of ACAMS will be considered by ACAMS as meeting its pre-qualification criteria for attempting the association's Certified Anti-Money Laundering Specialist (CAMS) examination. This course also qualifies for CE credits for CAMS certified ACAMS members. For more details on the UNSW AML course and about our chapter, visit our webpage at [www.acams.org.au](http://www.acams.org.au). 



## New York Chapter

**A**CAMS New York Chapter is proud to welcome its two newest executive board members! Hal Crawford of Brown Brothers Harriman & Co and Meryl Lutsky of the New York State Attorney General's Office were elected to the executive board at its December 2010 board meeting.

Crawford is the global head of anti-money laundering and the deputy director of compliance for Brown Brothers Harriman & Co., the oldest and largest partnership bank in the United States of America. He is responsible for oversight and direction of the firm's international AML and sanctions programs and participates in a variety of senior management activities designed to enhance firm-wide regulatory risk management control practices. He has more than twenty years of experience in global financial services, advisory and national bank supervision. His banking experience includes serving as the deputy regional money laundering prevention officer and head of financial intelligence at UBS Investment Bank in New York, the national director for enhanced due diligence at the US Trust Company of New York and compliance officer for Mid-Hudson Savings Bank. He spent several years working for Arthur Andersen's Regulatory Risk Services Practice, and was a national bank examiner with the Office of the Comptroller of the Currency (OCC). Crawford has long supported the New York Chapter and


hosted its mobile payments and electronic banking event in July 2010 at Brown Brothers Harriman & Co's New York headquarters.

Lutsky has been the chief of both the money laundering unit of the New York State Attorney General's Office and the New York State Crime Proceeds Strike Force since 2004. These units investigate and prosecute money laundering and its associated criminal conduct, as well as violations of the banking and tax laws. To investigate these complex crimes more effectively and creatively, she has assembled a task force consisting of federal and state prosecutors, law enforcement officers, and regulators. Among other cases, she has recently investigated several multi-state fraud rings whose crimes included identity theft, money laundering, credit card fraud, bank fraud and wire fraud.

Lutsky is also very active in educating and training financial institutions in how to protect their institutions from financial fraud. She participates in regional task force meetings throughout the state and meets with institutions on an individual basis to discuss their specific risk exposures and controls. She has also spoken about money laundering and related topics at numerous seminars and conferences, including the ACAMS Anti-Money Laundering Conference in Las Vegas, the West Coast Anti-Money Laundering Conference in San Francisco, the HIFCA Financial Symposium in New York, the

MAGLOCLN Conference in Columbus, and the ABA/ABA Money Laundering Conference in Washington D.C. For her work, Lutsky received the *AML Professional of the Year Award* at the ACAMS Anti-Money Laundering Conference in Las Vegas in September, 2010 and was featured in the previous edition of *ACAMS Today*.

Returning board members include co-chairs Barry Koch of JP Morgan Chase and Vasilios Chrisos of Macquarie Bank and board members Robert Goecks of EGRIS LLC, Allen Love of TD Bank, Denise Wright of RBC Capital Markets, David Chenkin of Zeichner Ellman & Krause LLP, James Stubbs of Citi, Dan Wager of the NY HIFCA, Erika Giovannetti of Morgan Stanley Smith Barney and Martin Feuer of Zurich Financial Services.

ACAMS New York Chapter has many interesting and informative learning events planned for 2011. The event in February on Cybercrime featured the writer James Verini, who authored the article *The Great Cyberheist* which was the featured story in the November 10, 2010 edition of *The Sunday New York Times Magazine*. If you are interested in joining the chapter or attending an event, please visit our webpage at [www.acams.org/ACAMS/ACAMS/Communities/Chapters/NewYork](http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/NewYork). Events are free to current chapter members! You may also contact us by email at [acamsnewyorkchapter@gmail.com](mailto:acamsnewyorkchapter@gmail.com). 

## Greater Boston Chapter


**I**n support of the ACAMS Greater Boston Chapter executive board's dedication to providing members learning opportunities that are of local and national interest, the executive board held a special session at the end of 2010. This session focused on planning out a year's worth of dynamic learning and networking opportunities. The events will provide chapter members with a balance of topics, presenters and forums throughout 2011. The format of the planned events includes a mix of breakfast meetings with formal presentations, evening chapter member-only networking gatherings, roundtable discussions led by a variety of subject-matter experts and an all day training

opportunity. The topics vary from law enforcement hot topics to bank related issues and from the domestic U.S. perspective to the state of anti-money laundering in Latin America.

The year kicks-off in February with a much anticipated case study presented by members of the Drug Enforcement Agency Money Laundering Task Force. John Grella of the Drug Enforcement Agency and Ryan Talbot of the Internal Revenue Service-Criminal Investigation focus the presentation on the black market peso exchange, the structuring aspect of money laundering and seizure warrants.

March brings a long awaited spring and the first of the ACAMS Greater Boston Chapter

networking events. An evening gathering at a favorite Beantown venue brings the opportunity for chapter members to have a free flow of ideas, open discussion and make contacts with other professionals.

If you are interested in attending these events, please join our chapter by visiting our webpage at <http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/GreaterBoston/Default.aspx>. If you have any questions about the chapter or any ideas or suggestions for events, please feel free to contact any of the executive board members listed on the web site or email [acamsboston@gmail.com](mailto:acamsboston@gmail.com). 



# Northern California ACAMS Chapter

We've grown by leaps and bounds!

Membership has increased to 120 chapter members since our launch on June 23, 2010 at the Marine Memorial in San Francisco. The executive board's goal is to increase membership to 150 during our 2011 membership drive by delivering relevant learning programs and exciting networking events in the Northern California AML community to help members deepen and expand their knowledge.

## Changes to the board

The Northern California ACAMS Chapter welcomes the latest additions and says goodbye to other members of the executive board.

In June 2010, chapter secretary, Eileen Monsurate and co-programming director, Natalie Ware sadly submitted their resignations to the board. We miss them and wish them success with their new ventures.

July 2010, we welcomed our new co-membership director, Bob Kenny of FinCEN.

November 2010, we welcomed our new chapter secretary, Erin Balbanian of Google, co-secretary, Elaine Laye, Legal Counsel for the FDIC and co-programming director Shawndra Rutledge, of Bank of the West.

January 2011, when he relocated to the Bay Area, we welcomed as our new co-communications director, Brian Stoeckert, former co-communications director for the Southern California Chapter's executive board.

## Learning events and program highlights

### 10/6/10 Virtual worlds and e-currencies

On October 6, 2010, ACAMS Northern California presented its first learning event of its inaugural year with *The Technology of Laundering: virtual worlds, cell phones, e-currencies — the world's new banks & AML's new frontiers*, presented by Mikhail Reider-Gordon, managing director of Litigation and Forensics of Capstone Advisory Group, LLC. More than 30 people attended this exciting event sponsored and hosted by Silicon Valley Bank in San Jose. Not only did attendees receive 2 CAMS credits, they also received a wealth of knowledge that directly related to the recent FinCEN proposal to

change the definition, under the BSA, of stored value programs.

One of the newest and least regulated trends is the use of virtual currency being used to commit crimes, including murder for hire. Virtual currency has become big business. In Hong Kong, the Octopus card is an anonymous rechargeable stored value smart card used by 95 percent of the population, generating over 11 million daily transactions worth over HK\$100 million (US\$12.8 million). This unregulated industry is now being accessed and used by devices such as cell phones, and wristwatches — even children's wristbands.

Final thoughts to this learning event are that banks are becoming less important because of newly emerging mobile platforms and mobile currencies. Telecommunication companies are increasingly providing financial services traditionally associated with "brick and mortar" banks. By using a pre-paid cell phone or a regular cell phone account, people can conduct most of their daily transactions via phone, often frustrating monitoring efforts conducted by financial institutions.

### 12/9/10 Toy Drive Benefit for Toys for Tots

Please see our press release on our Chapter Webpage.

Our year end event was a cocktail mixer at Bocanova Restaurant in beautiful Jack London Square. Several members attended this free networking event and sampled a variety of tasty appetizers and desserts. We held a toy drive to benefit our local community during this holiday season. We offer our gratitude for member support and to Alacra our sponsor.



Front row: Shawndra Rutledge, Perla Ortiz, Sandra Copas, Fran Falchook

Back row: John McCarthy, Ajit Tharaken, Howard Dilworth, William Voorhees, Jenner Balagot



Will Voorhees and Mikhail Reider-Gordon

### 1/27/11 The First Joint Chapter Learning Event In ACAMS History

The Southern California and Northern California Chapters joined forces to present the webinar *Understanding Offshore Tax Havens and The Impact of The New Tax Transparency Laws Mean for FIs*.

### Spanning the Globe: Best Practices to Comply with OFAC

Programming director Perla Ortiz and co-programming director Shawndra Rutledge are preparing a seminar geared to discuss the latest changes in OFAC sanctions, requirements, and best practices in enough detail to provide attending parties the knowledge necessary to take back to their organizations and review and/or improve their OFAC program.

In addition, as an added value, the session will provide fifteen to twenty minutes of impact analysis regarding Mexican regulatory changes. The change has been in effect for a few months — has it impacted the way we conduct business? Has there been a measurable impact to anti-money laundering efforts or the movement of illicit cash?

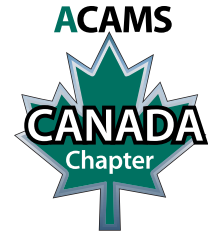
### Stay in touch

We would like to keep you informed of upcoming events, and chapter news. If you haven't already joined our LinkedIn Group please log on and add the ACAMS Northern California Chapter. You can also find details of future events on our chapter Webpage.

[www.acams.org/ACAMS/ACAMS/Communities/Chapters/NorthernCalifornia](http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/NorthernCalifornia) 

Sandra Copas, PI, CFE, Northern California ACAMS communications director, [scopas@copas-inc.com](mailto:scopas@copas-inc.com)





# Excellent attendance at second Canadian Chapter learning event

A thought-provoking panel discussion on key AML compliance issues was the focus of the ACAMS Canadian Chapter's second learning event.

The luncheon held on October 5, 2010 was attended by 130 participants. The luncheon built on the success of the chapter's first learning event and the presentation by assistant commissioner Mike Cabana of the Royal Canadian Mounted Police was well received.

The luncheon featured some of Canada's leading CAMLOs. It was graciously hosted by Anne Toal, CAMLO of Great-West Life, and Kirsten Lamertz-Harcourt, also of Great-West Life, at their Canada Life building in Toronto. The luncheon was sponsored by Lexis Nexis.

Event organizers wanted to provide participants with practical perspectives on issues


they might face on a daily basis. To make the event especially relevant, they drew on CAMLOs representing a cross-section of sectors.

The panel was moderated by Barbara Cox, vice president and chief anti-money laundering officer at BMO Financial Group. The panelists were comprised of Karim Rajwani, CAMLO at RBC representing the banking sector; Richard Hogeveen, CAMLO at Manulife Financial representing life insurers; and Derek McMillan, director, AML Compliance at Western Union representing MSB's and credit unions.

Topics of discussion included:

- New trends in the reporting of suspicious transactions, including tax evasion, corruption and human trafficking.
- How to control the quality of STRs

- The examination focus of FINTRAC, Canada's financial intelligence unit.
- Challenges in meeting sanctions requirements.
- How can the AML function add enterprise-wide value.
- Best practices in transaction monitoring.

The Canada Chapter is grateful to the hard work of the following members of its executive board who spearheaded organizing this event: Richard Hogeveen, chief AML officer responsible for Manulife Financial's AML/ATF program; Tim McNeil senior manager, Financial Intelligence Unit at the Bank of Montreal; Karim Rajwani, CAMLO at RBC; Garry Clement, president and CEO of Clement Advisory Group; and Kata Martinez, chapter development manager and task force liaison at ACAMS. 

# U.S. Capital Chapter

The U.S. Capital Chapter ended the year with a packed-house holiday networking event that set the stage for launching the chapter's 2011 calendar. The chapter is focused on developing enhanced multi-session learning events this year.

"We've had great learning events during the last year that have touched on topics of importance to our members," said Joe Soniat, chapter co-chair. "Past learning events have included AML law enforcement trends and emerging issues, criminal investigations and interviews with regulators and law enforcement. We have surveyed our membership and based on their feedback, we are going to take a more in-depth look at these topics. We also are going to increase our training events for money services businesses (MSBs)."

During the first half of 2011, the chapter plans to hold a three-hour training session for MSBs and financial institutions that do business with MSBs. Speakers are still being finalized,


but the sessions will include an overview of MSBs, a look at regulatory requirements for the industry, and ways to manage risk and build effective relationships between MSBs and financial institutions.

The chapter also is planning a day-long session with law enforcement that will provide an overview of emerging trends, case studies and explore the latest risks and trends in AML and CTF. "The chapter is working closely with the Special Investigations, Narcotics and Money Laundering Unit of the Fairfax County Virginia Police Department to develop this program," said John Byrne, chapter co-chair. "We are looking forward to offering a day of very interesting and high-quality sessions."

As with all chapter events, attendance to these learning events will be free to U.S. Capital Chapter members. More information on the events will be provided in the near future.

To help members build their compliance contacts, the chapter also will be holding six networking events this year. In response to member requests, the location for the happy hours will be rotated between Washington, D.C. and Virginia.

The chapter would like to welcome Don Temple, director of forensic, Advisory Services at KPMG, LLP, to the board. Don brings over 25 years of experience in the Bank Secrecy Act and anti-money laundering field. He has extensive hands-on experience in the areas of financial investigations including Federal income tax investigations, financial fraud, due diligence and anti-money laundering.

The chapter would also like to thank Monica MacGregor for her service as U.S. Capital Chapter membership director. Monica is rotating off the board after two years. She was one of the founding members of the chapter and has served since its inception. 




# Launch of the Edmonton ACAMS Sub-Chapter (part of the ACAMS Canada Chapter)

**A**nti-money laundering (AML) specialists from the Edmonton area and one member from the Calgary ACAMS regional working group ventured out on probably one of the coldest days this year to attend the first ACAMS Sub-Chapter event held at the Amber's Brewing Company. Despite one of the heaters not working, everyone enjoyed networking with other AML specialists.

The evening involved a short presentation by our event sponsor, Brad Chafer, account executive western region, from Lexis Nexis. The presentation focused on the Bridger Insight XG client identity management solution which is designed to assist with meeting AML compliance. Lexis Nexis was very generous in their promotional sponsorship which included giving away three copies of *A Guide to Canadian Money Laundering Legislation*, authored by Terence D. Hall.

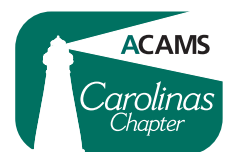
Following the presentation by Lexis Nexis there was a tour of the brewery and a beer tasting. The event went very well, everyone seemed to enjoy learning about the "Bridger

Insight" tool, the brew master's stories about money laundering in the bar industry and corruption in government, as well as the opportunity to taste different kinds of beer.

We have received favorable feedback about the event and we are planning our next event for February/March 2011. 



## Carolinas Chapter




**T**he Carolinas Chapter returned to the Queen City for its first meeting of 2011. Bank of America in Charlotte was the site this time as chapter chair, Bill Fox welcomed executive associate director of Homeland Security Investigations, Immigration and Customs Enforcement, James Dinkins. Dinkins, who leads the second largest criminal investigative agency in the United States, spoke to the group about ICE's mission and more specifically the growing problem of human smuggling and human trafficking and the role AML initiatives play in detecting and deterring this tragic crime. Dinkins shared statistics and

case studies of traffickers victimizing illegal aliens, women and young children and the public/private partnerships that in many cases are responsible for bringing these people to justice. Over 100 chapter members were in attendance to hear the presentation and provide their insight into AML trends in this field. "Human trafficking and its financial and societal costs cannot be ignored by financial institutions and ACAMS is providing a valuable resource in educating AML professionals in helping combat this crime," said newly appointed chapter co-chair Rob Goldfinger.

We look forward to more great events coming from the Carolinas Chapter in the coming months as we bring more quality training and networking events to the region.

For more information on the ACAMS Carolinas Chapter, please contact Rob Goldfinger at [RGoldfinger@sightspan.com](mailto:RGoldfinger@sightspan.com). Or, to find out how to get involved with this or any other chapter please contact Kata Martinez, ACAMS' chapter development manager, at [cmartinez@acams.org](mailto:cmartinez@acams.org)

Please visit the Carolina Chapter's webpage at <http://www.acams.org/Chapters/Carolinas.aspx>. 



## Southern California Chapter

The ACAMS Southern California Chapter closed out 2010 with a town-hall style learning event with local representatives from federal law enforcement and pressed into 2011 breaking new ground in ACAMS with the first co-presented learning event with another chapter.


On December 2, 2010, the chapter presented "Terrorist Financing in Southern California: Recent Cases and Trends." The event was held at the Elk's Lodge in San Gabriel, California and was followed by a holiday networking reception that was open to all ACAMS professionals. The panel included representatives from the Federal Bureau of Investigation, United States Attorneys' Office, Internal Revenue Service Criminal Investigations and United States Customs and Immigration Enforcement.

The panelists digested numerous instances of terrorist financing methods including trade based money laundering, international wire transfers through third party intermediaries, fund transfers with no logical connection to the originator or beneficiary and proceeds from the sales of counterfeit goods that were bulk cash smuggled through Asia and Mexico.

In an open forum with the panel, the audience of more than 70 attendees engaged in a question-and-answer session that expanded the scope of the event. The panel addressed topics that included how law enforcement agents use the Suspicious Activity Reports (SAR) submitted to FinCEN, the cash intensive nature of the Middle East, shell companies used to move illicit funds, human trafficking, bulk cash smuggling at LAX airport, and the underlying value of the supporting documents to a SAR in a money laundering prosecution.

More importantly, the panel stressed the importance and effectiveness of building relationships in the local financial crimes community. One panelist provided several examples of how relationship building with financial institutions greatly assisted with a federal seizure. Moreover, a panelist recommended anti-money laundering professionals read *Money Laundering: A Guide for Criminal Investigators*, second edition, by John Madinger, which provides a broad perspective on financial crimes, methods, case studies, and applicable laws.

To kickoff the 2011 program, the chapter developed the first co-marketed and branded learning event with another chapter. On January 27, 2011, the ACAMS Southern California Chapter and ACAMS Northern California Chapter partnered with DLA Piper LLP, a top international law firm, to present a web seminar on "Understanding Offshore Tax Havens and the Impact of the New Tax Transparency Laws for Financial Institutions." The two-hour web seminar earned attendees 2 CAMS credits for members of both chapters. Guest speakers included Alan Granwell, partner, DLA Piper LLP, Bruce Zagaris, partner, Berliner, Corcoran & Rowe LLP and James Dowling, director, Dowling Advisory Group. Mikhail Reider-Gordon, managing director, Capstone Advisory Group, LLC served as moderator.

Finally, in December, executive board member Brian Stoeckert was appointed by John Byrne, ACAMS executive vice president, as chair of the newly formed ACAMS Chapter Steering Committee, which will support planned, new, and existing ACAMS Chapters. 

## Chicago Chapter



In its ongoing commitment to provide continuing education, the Chicago Chapter of the Association of Certified Anti-Money Laundering Specialists (ACAMS) hosted a learning event on December 10, 2010 for its members. The event topic was helping to improve a caution list screening process, reduce false positives and address challenges associated with anti-money laundering (AML) transactions monitoring and tuning. Henry Balani, CAMS, managing director of Accuity's Strategic Services Group and Gregory LeMond, CAMS senior manager from Crowe Horwath LLP were the event presenters. Both speakers provided excellent guidance and suggestions to improve screening efficiencies and best practices to ensure closer adherence to current AML standards.


Balani provided specific and practical advice on how to reduce the number of false posi-

tives in the sanctions screening process. In defining and expanding upon key criteria such as entity types and sources, tokens, rules processing, and false negatives and positives. Balani's presentation covered the full spectrum of sanctions screening essentials. In addition, Balani shared valuable insight by offering best practice suggestions for dealing with screening anomalies, SWIFT data, and risk patterns. LeMond discussed the challenges associated with fine-tuning an AML transaction monitoring program and provided specific steps on how to address these challenges. By presenting detailed comparison analysis of transaction monitoring conditions and parameters within a standard AML program, LeMond was able to highlight the keys to successful development of monitoring solutions. The interchange of questions and responses between



Henry Balani of Accuity and Gregory LeMond of Crowe Horwath LLC

the speakers and attendees was enlivened, particularly given the relevance and impact of the material.

The Chicago Chapter also had a learning event in February and featured a three-speaker panel discussion on filing effective Suspicious Activity Reports. A number of events spanning a range of AML topics are already in planning stages, with scheduling slated through June 2011. For more details on past and future events, refer to the Chicago Chapter web site at: <http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/Chicago/Default.aspx>. 



# South Africa Chapter

Our mission is to “support the international ACAMS mission, advance the knowledge of local AML/CTF specialists, and provide a vehicle through which all local members can network and improve the level of AML/CTF understanding and effectiveness.”



## ACAMS South Africa chapter — news and updates

### Background to the chapter and launch:

The ACAMS South Africa chapter was officially launched in Johannesburg on the 3rd of November 2010 and sponsored by PWC. The South Africa board got together initially during February 2010 and started the process and discussions to launch by the end of 2010. With the assistance of various chapters, ACAMS U.S. and a tremendous amount of work and effort by the entire board the launch was a huge success. We also had the pleasure of having the ACAMS executive vice president John Byrne and Jose Lewis the regional manager Africa, Asia and Middle East at the launch. From a South Africa perspective we had Murray Michel the director of the Financial Intelligence Centre and various representatives from local law enforcement, the local and international banking sector, independent board of regulatory auditors, casino association of SA,



Murray Michel, director of the Financial Intelligence Centre



Academics from various universities, South African reserve bank, audit firms including KPMG, Deloitte, E&Y and PWC, the national prosecuting authority, The South African revenue service, insurance companies and many others.

### Key messages:

John and Murray delivered the key messages during the launch attended by approximately sixty delegates. The following is an extract of the key comments:

- How does ACAMS fit into the local environment and the impact it could have.
- The global threat of drugs, terrorism, human trafficking, weapons smuggling, counterfeiting, fraud and corruption.
- The flow of illegal funds throughout the global environment via various institutions.
- The South African government and stakeholder’s commitment in the fight against money laundering and related offences.
- Interdependence and cooperation required between the private and public sector in the fight against organised crime.
- Enhanced identification, monitoring and prosecution abilities.



John J. Byrne, ACAMS executive vice president

- Launch of ACAMS SA chapter is a milestone in the fight against crime in South Africa and greater AML compliance in all businesses will be accomplished through the CAMS certification process.
- Sharing of international best practice and intensive interaction with FATF.
- ACAMS SA will be the vehicle to attract AML experts from various and diverse industries.

### Growth of the chapter since the launch:

The ACAMS South Africa chapter is pleased to announce that the membership applications received from the launch on the 3rd of November 2010 until the end of January 2011 has reached 73. The board members have been inundated with requests for membership and additional information. The chapter has also committed to hosting learning and networking events throughout the year in both Johannesburg and Cape Town — see the chapter web site for more information. Recent developments include an ACAMS Africa conference to be hosted in Johannesburg during July 2011.

For more information on the ACAMS SA chapter including details on their mission, board composition, upcoming events and general information please visit their webpage at <http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/SouthAfrica/Default.aspx> or send an email to [acamssouthafricachapter@fcrmc.co.za](mailto:acamssouthafricachapter@fcrmc.co.za)

*Chris Steyn, communications director, ACAMS SA Chapter*

# The Richmond Chapter

The Richmond (Virginia) Chapter continued to grow during this past quarter. Its growth was helped along when a local television station invited chapter board members Elaine Yancey and Joe Soniat to participate in an on-camera interview. Joe and Elaine used the opportunity to discuss ACAMS, the Richmond Chapter, anti-money laundering efforts, how common a problem money laundering is and what investigators look for to expose it. The interview, which initially aired on November 8th, was later picked up by a National news agency. Both Joe and Elaine said the on-camera interview was an interesting experience. By the end of November the Richmond Chapter had grown substantially with members from both public and private sectors.

On December 9, the chapter held a complimentary holiday event at Eurasia Café &

Wine that included complimentary drinks and appetizers for members. This provided another great opportunity for members to socialize and network. The chapter also used this occasion to show support for the Central Virginia Food Bank, a worthwhile community cause.

As yearend grew near, the board met to carry out planning and organization of events for the coming year, which will include several learning and networking conferences. The chapter plans to continue its practice of attracting leading industry professionals to speak at their events. The Richmond Board would like to thank those who have already secured their memberships and invite industry professionals living in the Richmond and surrounding areas that have not already done so to become members. Chapter membership is

a cost-efficient way to gain CAMS recertification credits, obtain useful day-to-day knowledge and develop valuable industry contacts. 📺

## RICHMOND CHAPTER BOARD

R. Joe Soniat, Co-Chair  
 Elaine R. Yancey, Co-Chair  
 Elizabeth Vega (Lisa), Secretary  
 D. Scott Bailey, Co-Secretary  
 Donna Kitchen, Treasurer  
 Donna Thrift, Co-Treasurer  
 Charlie George, Membership Director  
 Diane Eisinger, Co-Membership Director  
 Fallon Teufert, Programming Director  
 Dr. Gurpreet Dhillon,  
 Co-Programming Director  
 Amy Wotapka, Communications Director  
 Dr. Thomas J. Burns,  
 Co-Communications Director

## MEET THE ACAMS STAFF

# ACAMS Operations Department

ACAMS Today had the opportunity to speak with Ericka Araujo, ACAMS business support coordinator. Araujo is the liaison for the ACAMS Asia office. Araujo's day-to-day duties include assisting member services with developing and enforcing member service policies and procedures to ensure consistent customer service satisfaction and processing certification/recertification applications.

Araujo is originally from Des Moines, Iowa and moved to Miami in 2007. Previous to joining ACAMS, Araujo worked for Wells Fargo Home Mortgage in West Des Moines, Iowa as a MAC Administrator/Administrative Assistant where she managed the fulfillment side of member services and assisted the director of operations.

Araujo has an associate's degree in Business Administration from Des Moines Area Community College and is currently working on completing her bachelor's in Business Administration.

**ACAMS Today: What has been the biggest improvement in the Association in the past three years?**

Ericka Araujo: In the past three years I have seen tremendous growth in membership. As a result of this phenomenal growth, ACAMS is continuously seeking ways to provide members with excellent member services, outstanding training and above all being a networking platform for the AML community. One of the most significant improvements has been the launch of more chapters and the updated web site.

**AT: What part of your job is the most rewarding?**

EA: Assisting our ACAMS members and helping them become CAMS certified.

**AT: What is your favorite part about ACAMS' conferences?**

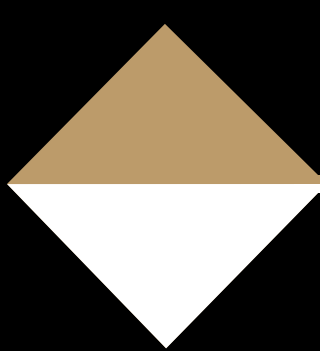
EA: I have the opportunity to work at the registration desk during conferences and



this is a plus for me because it gives me the opportunity to be one of the first people to meet the attendees. This allows me to put a face with the name of a member I may have assisted either by phone or email. I also like to attend the networking events and see the members' interaction with other members.

**AT: Where do you see ACAMS in the next five years?**

EA: In the limelight. ACAMS will continue to be at the forefront of training in the anti-money laundering field and continue to grow exponentially. 📺



# SIGHTSPAN®

Navigation for Business Information®

## AML/CTF Functional and Technical Expertise

Banking | Brokerage | MSB | Prepaid | Government

SightSpan, Inc. Dubai  
Office Building 3, Green Community  
Ground Floor  
Dubai Investment Park  
United Arab Emirates  
Phone: +971 (0)4 801 9254  
Fax: +971 (0)4 801 9101

SightSpan, Inc. USA  
Corporate Headquarters  
PO Box 4023  
Mooresville, NC 28117  
United States of America  
Phone: (704) 663 0074  
Fax: (704) 664 2807

SightSpan, Inc. Singapore  
UOB Plaza 1, 80  
Raffles Place  
Singapore, 048624  
Singapore  
Phone: +65 6248 4688  
Fax: +65 6248 4531

SightSpan, Inc.  
New York Office  
5 Penn Plaza  
19th Floor  
New York, NY 10001  
United States of America  
Phone: +01 212 849 6841

[www.sightspan.com](http://www.sightspan.com)