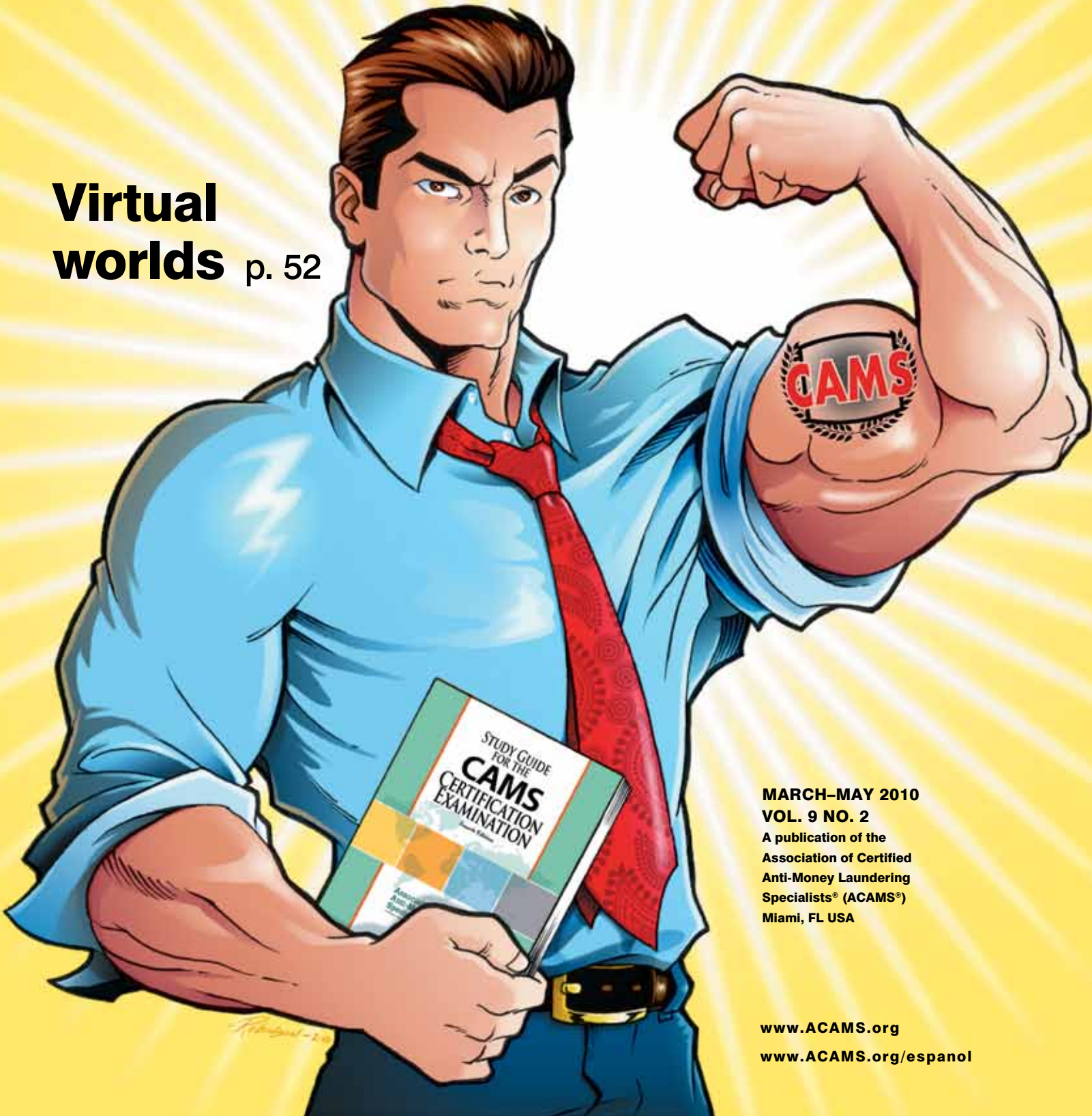


ACAMS[®] TODAY

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

Train like a champion p. 40

Virtual
worlds p. 52



MARCH-MAY 2010

VOL. 9 NO. 2

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

www.ACAMS.org

www.ACAMS.org/espanol

JAKE RANDALL IS A HARD WORKER.



BUT NOT MANY BARTENDERS OWN
BEACHFRONT ON MARTHA'S VINEYARD.

NEW WESTLAW PEOPLEMAP

Need to know who's working off the books? Westlaw® PeopleMap is the new tool that quickly helps you learn about people and their relationships to assets, public records, legal filings – and other people. Before you've even started your research, PeopleMap has made relevant connections between people from billions of records across the country. So you can find out what you need to know now. **Westlaw PeopleMap: what's in a name might surprise you.**

To learn more, visit west.thomson.com/peoplemap or call 1-800-762-5272.



Regulatory pressure is growing, but your budget isn't.



With evolving AML regulatory requirements - transaction monitoring, Know Your Customer (KYC), and sanctions/watch list filtering - financial institutions are challenged to meet their growing compliance obligations while managing available resources and long-term costs.

Actimize has a deep understanding of these challenges and is helping leading financial institutions across the globe - including retail and investment banks, brokerages, and insurance providers - meet ongoing compliance needs with a comprehensive suite of AML solutions.

Our solutions save our clients time and money, and have been proven to produce half the number of alerts over competing solutions. Actimize's core technology platform provides advanced analytics and monitoring capabilities, which have been enhanced through the acquisitions of Fortent and Syfact. Actimize empowers your organization with the flexibility to efficiently and cost-effectively adapt to dynamic regulatory and business requirements.

Contact us today to learn more about how we can help your organization: info@actimize.com



ACTIMIZE
a NICE company


www.actimize.com

New York:
212-643-4600

London:
+44 (0) 20 7255 1065

Japan:
813-5408-9050

Hong Kong:
852-2598-3838



“ AML RightSource’s team of compliance professionals provide the manpower we need to make sure the important elements of our BSA/AML program are being addressed on a daily basis.

Working with AML RightSource allows us to focus on making our institution more profitable.”

*-Blackhawk Bank
Wisconsin*

*Visit us on the web to hear more from Blackhawk Bank
<http://www.amlrightsourc.com/testimonial>*

My solution ... the **SMART** solution.

WHAT'S THE REAL COST OF YOUR BSA/AML PROGRAM?

Outsourcing with AML RightSource, streamlines transaction monitoring, customer risk profiling, FinCEN reporting and more. Whether you are a large bank holding company or a local community bank, let AML RightSource analyze your BSA/AML program to design a cost effective solution for your institution.

Let AML RightSource do the work so you and your team can focus on the business of banking.

ACAMS

Executive Vice President: John J. Byrne, CAMS
Editor/Communications Manager: Karla Monterrosa-Yancey, CAMS
Global Director of Conferences and Training: Eva Bender
General Manager: Kathleen Richardson
Senior Vice President of Business Development: Geoffrey Chunowitz, CAMS
Director of Asia/Pacific Region: Hue Dang
Director of Operations for Latin America: Gonzalo Vila, CAMS
Marketing Manager: Kourtney McCarty
Certification Manager: Giovanna Oquendo, CAMS
Account Executives: David Kehr, Sonia Leon, Camila Levy and Jose Lewis
Corporate Sponsorship and Advertising: Andrea Winter
Graphic Designer: VR Fischer

ACAMS ADVISORY BOARD

Richard A. Small, Chairman, Enterprise Wide AML and Sanctions Risk Management, American Express, USA
Alberto Ávila, CAMS, Executive Director, COMLAFT, Mexico
Samar Baasiri, CAMS, Head of Compliance Unit, BankMed, Lebanon
David Clark, CAMS, Head of Financial Crime Intelligence and Analysis, Barclays Wealth Financial Crime, UK
Susan Galli, CAMS, Chief Risk Officer, Pacific National Bank, Miami, FL, USA
Peter Hazlewood, Managing Director Compliance Services & Security Group Legal, Compliance, Secretariat and Security, DBS Bank, Hong Kong
Michael Kelsey, CAMS, Global AML Director, Capital One, Richmond, VA, USA
William D. Langford, Senior Vice President and Director of Global AML, JP Morgan Chase and Co., New York, NY, USA
Anthony Luis Rodriguez, CAMS, CPA, Chief Global Compliance Officer, RIA Financial Services, Cerritos, CA, USA
Nancy Saur, CAMS, FICA, Regional Head of Compliance & Risk Management, ATC Group N.V., Cayman Islands
Markus E Schulz, Chief Compliance Officer Global Life & Banking, Zurich Insurance Company Ltd, Zurich, Switzerland
Daniel Soto, CAMS, Executive Compliance Director and BSA Officer, GMAC, Inc., Charlotte, NC, USA

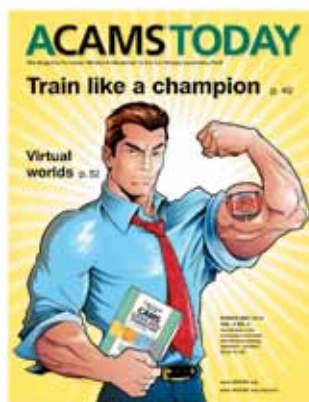
ACAMS Today is designed to provide accurate and authoritative information concerning international money laundering controls and related subjects. In publishing this work, neither the authors nor the association are engaged in rendering legal or other professional services. The services of a competent 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
 E-mail: info@acams.org
 Website: www.ACAMS.org • www.ACAMS.org/espanol

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

ON THE COVER



Train like a champion p. 40

From the editor 6

CAMS graduates 6

Member spotlight 8

A message from the Executive Vice President 10

Expert spotlight 12

The nexus between financial crime, money laundering and terrorist financing 16

Too good to be true? 18

The trouble with SARs 22

Climate change and the risk of money laundering 24

The UBS case 28

Money laundering then and now 30

New Jersey and you 34

The Eastern African Community (EAC) 36

Train like a champion 40

Consolidated FIUs save institutions time, money and headaches 42

Developing the investigative mind 46

Collective Entity Resolution 48

Virtual worlds 52

Meet the ACAMS staff 55

Know Your Chapter 56

Events calendar 62



November-January CAMS Graduates



I am a bit of a sports fanatic. I grew up watching and playing soccer, tennis and basketball with family and friends. Needless to say, as I am writing this article we have had some impressive sporting events occurring. One of those spectacular sporting events happened right here in Miami — the Super Bowl — need I say more?

Currently, I am fixated on watching the Winter Olympics. I have always been impressed by athletes who train their whole lives for that one pinnacle

moment — bringing home the gold.

What do all these successful athletes have in common? They train like champions. A champion is defined as a person who achieves excellence. The lead article: *Train like a champion* discusses how you can have a championship anti-money laundering (AML) program by training your *athletes* (employees) like champions.

Too good to be true? This is the title of the article dealing with hedge fund AML risk and if it seems too good to be true, odds are that additional due diligence is needed.


Political corruption can be found nearly everywhere around the globe. *New Jersey and you — perfectly corrupt together* focuses on the reasons why political corruption is so prevalent in New Jersey and it discusses the indicators of fraud and money laundering.

With the success of the movie Avatar at the box office, more and more of the mainstream community is becoming familiar with virtual worlds and the origin of avatars. *Virtual worlds: A tool for money laundering and terrorist financing* discusses vulnerabilities with virtual worlds where the money laundering and terrorist financing criminal can capitalize. Learn best practices you can implement to mitigate risks associated with virtual worlds.

Also, we would like to welcome our new Executive Vice President, John J. Byrne, CAMS. John's reputation precedes him within the AML community. Meet the Miami staff and discover what John's vision and goals are for ACAMS in the Executive Vice President's letter.

Finally, if you're interested in expanding your knowledge and earning continuing education credits, don't forget to register for upcoming ACAMS Web Seminars by visiting the ACAMS web site at www.acams.org.

As always, if you prefer to read us in Spanish, you can visit us at www.acams/espanol.org to download an electronic format of *ACAMS Today* "en español."

And don't forget to send your comments, ideas for articles and submissions directly to me at editor@ACAMS.org. 

Karla Monterrosa-Yancey, CAMS
Editor/Communications Manager
ACAMS

- | | |
|--------------------------------|-----------------------|
| Nathan | Adderley |
| Nirla M. | Afenir-Ratanapeanchai |
| Kavinda | Agalawatte |
| Adekunle | Ajiboye |
| Khaled M. | Al Tamimi |
| Farouk | Alaryan |
| Houssam | Al-Humaidan |
| Alissa Joy | Allen |
| Husain S. | Almudaifa |
| Belkis | Amaya Gonzales |
| Michal | Amzallag |
| Rebecca | Anderson |
| Daniel Ernesto | Angulo Parra |
| Jay | Arnett |
| Fatima Hasan | Ashoor |
| Royce | Askew |
| S.M. | Astaquzzaman |
| Suzanne | Atwood |
| Rodrigo Sebastian Del Transito | Avendaño Salgado |
| Mohamed F. | Awad |
| Carlos | Ayala |
| Arthur | Babayants |
| Jay H | Baker |
| Babita | Balan |
| Chalo | Balandran |
| Wilfred | Barboza |
| William | Barry |
| Christopher | Baum |
| Karen | Beauchene |
| Sandra | Behar |
| Jane | Bell |
| Engelberth Antonio | Beteta Gonzalez |
| Charles R. | Blackburn |
| Jennifer | Blake |
| Christopher D. | Blanchette |
| David E. | Bliss |
| John | Bodsworth |
| Paula | Borges |
| Gary | Brennan Jr |
| Ashley | Brewer |
| Melissa E. | Brudzinski |
| Tracy | Bruner |
| Cerica | Buhat |
| Yasmin Rahman | Bula |
| Razaak | Busari |
| Shane Talbot | Campbell |
| Christine N. | Casanova |
| Veronica | Casian |
| Cesar Ivan III | Cazares Cuevas |
| Glendy Chung Yan | Chan |
| Pik Fai | Chan |
| Selina Chor Wah | Chan |
| Jacky Tsz Yeung | Chan |
| Calisa | Chan Si Wai |
| Andres | Chapellin |
| Reshma | Chaturvedi |
| Ajay Kumar | Chauhan |
| Luis Miguel | Chavez |
| Winnie Wing Yee | Cheung |
| Desmond | Chew |
| Sammy S.B. | Chilunga |
| Carmen | Chin |
| Lee Lee | Choi |
| Sharen Chai Lee | Choo |
| Wing Kin | Chow |
| Meghan | Clark |
| Ricky L. | Clark |
| Ned | Cohn |
| Valerie | Collier |
| Donna | Coniglio |
| Matthew L. | Conover |

Catherine Contreras
Lilium M. Cordero
Maria Laura Crotti
Chaitanya Dalvi
Bradley Davis
Rosanna Deamer
Anne DeFrehn
Alan Dickson
Ousmane Dieme
Kristen Dwyer
Russell C. Easley
Sine Amyta B. Edal
S Sunil Edwards
Robert Enzaldo
L Michael Ewald
James Femia
Jason M. Ferguson
Brooke Ferris
Thomas A. Finati
Alexis Flores
William N. Florian
Mo Yun Fong
Nancy Fraher
Richard Fraser
Michael Froncek
Chi Luh Fu
Elmi Gabobe
John E. Galjanich
Chris T. Galloway
Kim Garbino
Michael Giacoppi
Laura H. Goldzung
Jenny Alexandra Gomez Sarmiento
Graham R. Gorrie
Christopher M. Graham
Bobby Lee Griffin Jr
Shanna S. Hall
Prasanna Haran
Mohammad Mahbub Hasan
Yuka Hayashi
How Hee Peng
Enrique Alfonso Hernandez Rivas
Kai Tat Ho
Donald K. Hoover
Sumita Hore
Yoko Hoshido
Kamal Hossain
Paul Hoyer
Cecilia Hoytink
Aurobrata Hui
Cristiane R. Hume
Shadner Anthony Ifrene
Kerstin Irwin
Muhammad U. Izhar Qureshi
Rigoberto Jacome
David Jansen
Ali Jessa
Peggy Jimenez
Roberto Jimenez
Timothy P John
Corinne Johnson
Tina L Jones
Shane Jordan
Deb Jost
David W Jourdan
David Kaawa
Raj Kadakia
Sara Kalban
A.K.M Rezaul Karim
Amit Vasant Karode
Rita Kaslof
Perminder Kaur
Elizabeth Kay
Michael D. Kelsey
Mee R. Kim
Eunice J. Kiptoo

Rizwan Kirmani
Brandie Klee
Brandon Klerk
Brian Kloostra
Justin Koenig
Stephen Korinko
Keiko Koshino
Gwyn Langborgh
Shawn Lawless
Domyung Lee
Freddy Kuang That Lee
Lin Mei Lee
Gregory Lemond
Chee Keong Leo
Carol Ann Levesque
Yong Li
Huey Yong Lim
Jiun Sandy Long
Angela Paola Losada Rivera
Randy MacDonald
Susan Machala
Melissa Mack
Joyce Madden
David R. Madrid
Tariq Mahmood
Paula L. Mango
Laura K. Maroncelli
Julio Cesar Marono
Stacy Marrufo
Brigitte Martinez Fernandez
Abrar M. Masud
Sara McGinnis
Ian McInerney
Tyler L. McNally
Erica J. Meissner
Vince Micieli
Catherine L. Mieczkowski
Evelyn Miller
Patty Mills
Golam Mohiuddin
Shawn D Moore
Joseph Moritz
Patrick Mukubonda Lilungwe
Mark J. Mullen
Zubin Nitin Muriya
Anandan Murugesan
Krishnan Muthurathinam
Marietta Myrold
Cosmin Nare
Ndeye Nguenar Ndao
Taryn W. Nelson
Kate B. Ng
Dianne Nguyen
Sergei Nilov
Orlando Olivares
Wanda Ortiz Navarro
Kim W. Palermo
Jose M. Patin
Jamone Patterson
George Pearson
Gabriel Pena
Alan G. Perkins
Wayne H. Peterson
Atuweni-Tupichile Phiri
Astrid Liliana Pinzon Fajardo
Timothy J. Potero
Rosemarie G. Prado
Christa Price
Carmela Pulido
Michelle Quon
Rahul Raghavan
Sowmya Rajamani
MD Masud Rana
Adbur Rauf Shaikh
Kjellin Rawlins-Elliot
Nicole L. Relyea

Josephine Reyes
Allen Lee Roberts
Allen Robin
Johnny Rodgers
Pamela Rodriguez
Mirna Rodriguez
Joanne Roldo
Christian Alberto Rosales Morales
Jaime Rosenman
Suraiya Rowley
Rajagopal Sampathkumar
Benjamin Sanders
Maria Conceicao Santos
Marwan Satti
Jeanne Schurott
Marybeth J. Schwanger
Andrew Sealey
Irine Seo
Kevin Seymour
Naim Shaikh
William E. Shea
Alejandro V. Shea
Miaoqing Jayne Shee
Lynn Shen
David Sheppard
Rob Shoemaker
Carol A. Shortall
Matthew D. Shovein
Bishara Shubeita
Donald A. Silas
Asmita Singhi
Mark Siska
Daphne Tak Yi So
Peter Stangert
Kristinn Stefansson
Anthony Steo
Gokulnath Subbarao
Stacy A. Surat
Catherine Sutcliffe
Benjamin David Sutherland
Kristofer L. Swank
Ma. Cecilia F. Taliman
Melisa Tan Hwee Joo
Robert Tetreault
Janet Thompson
Charlene Thompson
Alexander Thompson
Juan Carlos Torres Pabon
Trevor A. Trim
Susan Trpcevski
Beth E. Trueman
Christopher S. VanHuyse
Vinod Vadakkekottoor Varghese
Balaji Venkatasubramanian
Kimberly A. Via
Brian L. Ware
Alexander Warr
Catherine Webb
Hayley Webster
Don t Wedderburn
John Wells
Jamy Wheeler
Gregory A. White
Stephanie L. Whitten
Erin L. Wilson
Julie Wilson
Brandi Wolfinger
Elizabeth J. Woltz
Pui Kie Wong
Cheryl Wright
Kevin Leslie Wright
Luning Ye
Vsevolod M. Yegorov
Jeffrey Yuk
Xin Zhang

MEMBER SPOTLIGHT



Kunda Emmanuel Kalaba,
CAMS
Lusaka, Zambia

Kunda Kalaba is the third Zambian National to be awarded the CAMS credential after Professor Kenneth K. Mwenda in 2005, and John Machayi 2009.

Kalaba is currently the Country Head of Financial Crime Risk Department – Standard Chartered Bank Zambia Plc, and is accountable for the Financial Crime Risk management framework in the country. Upon obtaining the CAMS certification, he was appointed as Country Money Laundering Prevention Officer (CMLPO) and among many other assignments is responsible for providing leadership and direction and ensuring that the in-country anti-money laundering (AML) efforts are in place. In addition he oversees that policies and standards are complied with, by professionally managing relations with law enforcement and regulators.

Before joining Standard Chartered Bank, Kalaba worked as Institutional Reform and Portfolio manager. He was responsible for institutional reforms, capacity building, promoting sound economic governance transparency and accountability.

Previously, Kalaba was a manager in fraud prevention in the Investigations and Security Department with Barclays Bank Zambia Plc. He was responsible for Corruption and Fraud Detection, Prevention, Investigations, Security and Anti-Money Laundering activities within the Head Office, Divisions and all Branch network.

Upon graduating with a Bachelor of Arts Degree (Education) from the University of Zambia, Kalaba worked from January 1991 to January 2000 as Head and Senior Corruption Prevention and Investigations Officer with the Anti-Corruption Commission (ACC) in Zambia.

Kalaba has more than 19 years of hands-on extensive experience in sectors covering all financial crimes, anti-corruption, AML, Counter Terrorist Financing (CTF), banking operations, fraud and operational risk assessments, fraud examination and prevention measures, forensic investigations, bank and physical security, Corporate Governance, capacity building, Institutional Reform, Organizational development, business process analysis,

business process re-engineering and Regulatory reforms.



Yan Lixin
Shanghai City, China

Dr. Yan Lixin is one of the Founders and Secretary-General of the China Center for Anti-Money Laundering Studies (CCAMLS) at Fudan University, Shanghai, China. Through his dedication and efforts, CCAMLS and ACAMS were able to sign a partnership agreement in May 2009 to promote AML education in China. He was also instrumental in leading Fudan's efforts to translate the ACAMS certification program materials into Chinese. He is currently a CAMS-candidate and recently completed ACAMS's inaugural Train-the-Trainer Program held in Hong Kong which grants accreditation to selected candidates of bilingual capabilities to conduct the CAMS Examination Preparation Course.

He successfully organized the first national seminar on anti-money laundering in 2006 and the Second National Summit Forum on AML and CTF in 2009. He holds a post doctorate of Communications degree, a PhD of Economics, a MBA and Bachelor of Arts in English. He has written, compiled and translated more than 50 essays, theses and books published in well-known newspapers, magazines and periodicals, among which the "Basic Course on AML" and "Study on the AML Mechanism in Banks" are very influential.



Chris Smith
Hong Kong, China

Chris Smith has spent the past 25 years in the corporate security environment, in the UK, Africa, Europe and the Middle East. He has worked for international hotel groups and financial institutions. His current role in HSBC, as the Head of Regional Security & Fraud for Asia Pacific involves financial crime risk, information security risk, physical protective security, business continuity management and security intelligence.

Smith is a Steering Group Member of the Asia Crisis and Security Group, Chairman of the OSAC Steering Committee for Hong Kong & Macau, a member of ASIS International, a member of CSO Roundtable, a member and past

Co-chairman of the Asia Sister Banks Group and a Fellow of the Security Institute of the UK. He is a Board Certified Protection Professional and has a master's degree in crime risk management.

Smith is a member of the Asia-Pacific Task Force, and played a key role in providing input in the development of the 2nd Annual AML/CTF Conference program. He also contributed to the growth of ACAMS in Hong Kong by selecting key staff to enroll in the ACAMS certification program.


Salvatore Zerilli, CAMS
Princeton, NJ, USA



Salvatore Zerilli, CPA, CAMS is a principal in Mercadien, P.C., CPAs and a managing director of The Mercadien Group.

A seasoned public accounting professional, Zerilli specializes in performing outsourced internal audit services for community banks and US branches of foreign institutions. Such services comprise an array of internal audits which are inclusive of the Bank Secrecy Act (BSA)/USA PATRIOT Act, allowance for loan and lease losses, asset/liability management, liquidity management, information technology, and regulatory compliance, among others.

The government instituted the USA PATRIOT Act in 2001, which placed further regulatory guidelines on the banking industry. Soon thereafter, Mr. Zerilli became a Certified Anti-Money Laundering Specialist (CAMS). Zerilli works with financial institutions to ensure that they have properly implemented compliance programs which meet the scrutiny of federal and state regulators. Well-versed in the various software applications for BSA compliance, Zerilli is a sought-after expert in this area.

Armed with more than a decade of banking industry experience and a B.S. in Accounting from the University of Albany (magna cum laude), Zerilli is a member of the NY State Society of CPAs and the American Institute of CPAs. He is also an active member of the Financial Managers Society (NY/NJ and Philadelphia Chapters) as well as an active member of the Association of Certified Anti-Money Laundering Specialists. 

2nd Annual ACAMS Anti-Money Laundering & Counter-Terrorism Financing Conference Asia Pacific

JW Marriott Shanghai, Tomorrow Square
Shanghai, People's Republic of China

Pre-Conference Workshops **26 April 2010**

Main Conference **27-28 April 2010**

Developing a World-Class AML/CFT Program

Don't miss this opportunity to:

- Meet AML/CFT experts from the U.S., China and throughout the Asia Pacific region
- Learn to navigate the nuances of multi-jurisdictional regulations
- Mitigate the risks of politically exposed persons
- Benchmark your AML program against your peers around the world
- Hear multiple in-depth case studies on solving real-world challenges
- Prevent the flow of illicit funds through your organization

Platinum Sponsor:



Media Partners:



A MESSAGE FROM THE EXECUTIVE VICE PRESIDENT

To the ACAMS Community:

It is a distinct honor to have this opportunity to serve as the Executive Vice President of the Association of Certified Anti-Money Laundering Specialists (ACAMS) and advocate for the broad membership that comprises the anti-money laundering (AML) community. My commitment to you is to continue the excellent leadership of ACAMS provided by Gregory Calpakis and before that, Saskia Rietbroek. Gregory's stewardship of the organization leaves us in terrific shape and it will be up to me, with considerable help from all of you, our Advisory Board, the chapters and the various task forces, to keep up the momentum. Most importantly, the tremendous staff here in Miami will make continued success an easy goal.

I have been fortunate to have been a part of ACAMS as a Board member since its inception in 2002, and most recently as Chairman. The concept of certifying the expertise of AML professionals in both the government and the private sector, created by Joy and Charlie Intriago, has turned into a 10,000 member organization with global credibility. That has never been clearer to me than during my 2009 and 2010 visits to Hong Kong, Taiwan and Australia. This success must be sustained and expanded, an ongoing goal that can only be achieved by responding to the membership and your needs. As a participant in this great organization, and with my twenty-two years at the American Bankers Association, I know that an association is only as good as its members. I will constantly reach out to this vast ACAMS community and seek your advice, counsel and assistance.

I know you will respond.

If you have visited our web site recently, you know that our mission statement, "to advance the professional knowledge, skills and experience of those dedicated to the detection and


prevention of money laundering around the world, and to promote the development and implementation of sound anti-money laundering policies and procedures," is only part of our direction.

ACAMS is acutely aware of the importance of sanctions, all forms of financial crime, and corrupt practices as necessary areas of subject-matter expertise for the AML professional. We will ensure that our programming includes those issues, and any other related areas where our members seek our assistance.

In future communications, after I have had an opportunity to speak to many of you, I will outline our short and long term priorities. Suffice it to say, I am committed to membership retention, chapter growth and advocating for you so that your voices are heard.

For now, I leave you with a view of my approach to challenges. Many who know me know I enjoy history and revisiting relevant quotes. One of my heroes, Senator Robert F. Kennedy, often referred to a quote from a play written by George Bernard Shaw when making the point of pursuing new approaches. The paraphrased quote, "There are those that look at things the way they are, and ask why? I dream of things that never were, and ask why not?" has always resonated with me because in the parlance of today, we need to think outside the box.

With your help, ACAMS can grow and improve to assist the AML professional as he or she grapples with our many challenges.

Please feel free to send me your thoughts and recommendations at jbyrne@acams.org or at 703-282-4954. 



John J. Byrne, CAMS
Executive Vice President



Miami Staff

ACAMS 9th Annual International Money Laundering Conference

Mandalay Bay | Las Vegas

Pre-Conference Workshops **September 19, 2010**

Main Conference **September 20-22, 2010**

Expanding the AML Lens: Compliance Strategies for a Global Economy

This year's fully updated program offers:

- Straightforward guidance on international laws and emerging US regulations
- Tools to optimize your AML department within a global economy
- Practical takeaways that will immediately improve your compliance program
- Reliable techniques for spotting the latest money laundering schemes
- Networking opportunities with industry peers and AML experts

Media Partners:



Asia Pacific and AML

The legislative regimes for anti-money laundering (AML) in the various countries in the Asia Pacific region are in varying stages of development and enforcement. These differing regimes present enormous challenges to banking institutions, whether they be domestically-focused, regionally-focused or global operations.

In emerging anti-money laundering (AML) regimes such as that of Mainland China, the filing of suspicious transaction reports (STRs) are entirely rules-based, while in more established AML regimes such as that of Hong Kong, STR filings are suspicion-based. These fundamental differences do present an enormous challenge to banking institutions that must comply with not only local filing requirements, but must balance those requirements with globally-established policies and procedures within their own institutions. Other compliance challenges include varying

requirements of know your customer (KYC) and customer due diligence (CDD), as well as compliance with local sanctions lists and databases coupled with international lists from Office of Foreign Asset Control (OFAC) and the United Nations.

It is against this backdrop that ACAMS recognized the need for an on-the-ground presence in Asia, and established its regional head office in Hong Kong in December 2008. Since then, ACAMS has seen phenomenal growth in the Asia/Pacific region in terms of membership and partnerships. The over-arching goal of ACAMS is to foster an AML community between the key stakeholders on AML issues, whether they are from the government sector such as regulators and law enforcement or private sector such as financial services institutions and gatekeeper institutions. The encouragement of such dialogue between the parties can only assist in mitigating the AML risks

inherent in all financial systems. It is with this vision of fostering the AML community that ACAMS organized its 2nd Annual Asia Pacific AML/CFT Conference in Shanghai, 26-28 April 2010, co-organized with our partner, Fudan University and with the support from the People's Bank of China. The event brings together regulators from the U.S. and Asia, including Bank Indonesia and Thailand's FIU, as well as industry practitioners from global financial institutions such as Standard Chartered Bank, Citibank, DBS, and Morgan Stanley.

ACAMS caught up with two influential individuals in the AML/CFT field for a combined-informative interview. Mr. Peter Hazlewood, Managing Director, DBS Group and Ms. Hue Dang, Regional Head & Director, Asia Pacific, spoke with *ACAMS Today* regarding the recent AML/CFT developments as well as the AML challenges facing Asia/Pacific region.



Peter Hazlewood

ACAMS Today: Describe your current position and responsibilities?

Peter Hazlewood: I work for DBS Group, the largest financial services group in South East Asia. DBS is headquartered in Singapore with operations in 50 cities within 16 markets.

I am currently the Managing Director, Group Compliance Services and Security; reporting to the Group General Counsel and I manage a team of over 100 employees. I have direct responsibility over all areas of financial crime, crisis and security risk management, including: Group AML/CFT compliance, transaction surveillance, training, Group Investigations, Group Security, Group Business Continuity Management, card fraud risk management, business practices investigations (mis-selling) and business intelligence.

AT: How did you first become involved in the compliance field?

PH: I started out as a police officer in Hong Kong in the 1980s working regular street crime. In fact my favorite role to date was the Vice Squad in Shamshuipo, Kowloon. When money laundering first became 'an issue of note' in the late 80s, I was fascinated by it and started to take an interest. As soon as I was able to, I went through money laundering investigation and asset tracing training with the Narcotics Bureau.

I specialized in white collar crime with the Commercial Crime Bureau and handled many complex international cases. In 1994/1995, I was part of the team that successfully brought the first shell bank prosecution in Asia (and possibly one of the first in the World). The bank's name was the Agriculture and Commercial Bank of Cambodia. I was the undercover officer who attempted to launder money through the shell bank.

In 1996, I was fortunate enough to handle — and successfully prosecute/recover assets relating to — an interesting case for JP Morgan's Private Bank. As a result, the head of Corporate Security recruited me to work for the Security Department in Asia.

About a year later, a compliance officer in Singapore asked me if I could design some new KYC policies and deliver AML training because I was really the only one in any of the Asian risk management functions that had any exposure to money laundering back then.

Fast forward a few years and JPM merged with Chase. My function was split into three: fraud and investigations went to Audit, security went to Real Estate and AML/sanctions went to Compliance. I was given a choice as to which path I wished to follow and I chose AML.

Finally, a former colleague from JPMC who had been appointed as General Counsel at DBS, asked me if I would consider returning to Asia (from New York) to set up an integrated financial crime, security and crisis management function. For me, this was a dream opportunity and here I am.

AT: Congratulations on being appointed as part of the ACAMS Advisory Board. As a new board member what are you doing in conjunction with ACAMS to help fight money laundering in the Asia Pacific region?

PH: We are launching ACAMS across Asia with a view to build awareness of financial crime issues and raise

compliance standards — especially in emerging markets. For example, last week, I had the honor to partner with ACAMS in the Taiwan launch and in April, we are partnering again in Shanghai for the second ACAMS Asia Conference. In Hong Kong ACAMS was launched with the first Asia Pacific conference and in Singapore, ACAMS teamed up with the recently launched Compliance Professionals Association so that ACAMS courses may be accredited and easily accessed via the Association. Actually, there is so much going on here in Asia that my head is spinning! Hue Dang, the excellent ACAMS Director of Asia/Pacific, is constantly innovating and extending the reach of this organization.

AT: What are some of the critical AML issues facing compliance professionals in the Asia Pacific region?

PH: Different regulatory approaches in the various Asian markets present a huge challenge if you aspire to have a consistent integrated group-wide model (as Basel would suggest). The vast array of different languages and cultures and the even more vast population is also a challenge, to say the least. Let's not forget that three of the five most populous nations on Earth are in Asia: China, India and Indonesia. For example, there are almost 70 million public sector employees in China alone. Think about that from the perspective of identifying and monitoring PEP accounts! The language issue wreaks havoc with surveillance systems and core banking platforms. It requires a real focus on detail in setting up operating procedures.

With the downturn, I would also say that loan sharking has once again reared its ugly head requiring the focus of all socially responsible banks and there is the

ever present concern about corruption in underdeveloped or developing markets.

But above all, the one thing that AML professionals really need to focus on in Asia is managing the risk of foreign sanctions — especially EU and OFAC, given that the USD and Euro are the world's clearing currencies.

AT: What do you find to be the key to success in the AML/CFT field?

PH: *Knowledge and experience:* Is the start point — not just of law or regulation, but real operational experience. You cannot manage the risk associated with an activity that you do not understand, and that knowledge needs to stay current.

Be patient: This is a big lesson I have learned!

Empowerment: As financial crime leaders, we need to be empowered to effect change and the governance model must clearly reflect such. Without empowerment we will only become bogged down in territorial issues that do not serve the interests of our shareholders and customers.

Simplicity: If you are tasked with a particular bit of the AML program, look at the task from the end-user, customer and shareholder's perspective, not your own and keep your solution simple (i.e., globally applicable CIP/KYC procedures), a single case management/business intelligence database, one enterprise transaction surveillance system for all financial crime activity, global AML training standards, single point of issue escalation per country, etc.

Network: You need to have a network: regulators, law enforcement, fellow financial institutions, vendors, academics and compliance educators.

AT: What advice would you give AML professionals for career growth?

PH: I am very fortunate in that I was able to get into AML pretty much at the beginning and grow with it, acquiring knowledge and experience as I went. When I first started, there was only one commercially available transaction surveillance system. Now, there is a mind-numbing array of things to learn.


If I were to advise a friend on this field, I would first urge them to choose their employer carefully. No amount of money will compensate you for working in a bad culture. Is the employer proactive? Do they invest in AML infrastructure when they are not under consent orders? Is it instinctive that that front office folks 'do the right thing?' Do they participate in ACAMS, etc.?

Secondly, having worked in Hong Kong, Singapore and New York I would say that international experience really does develop you quickly and makes you well rounded. It also builds a network. Don't be frightened to volunteer!

Thirdly, once you have chosen your organization and you have been tasked with a role, stick to it for enough time to actually achieve something meaningful. This may involve turning down better paid positions in the meantime, but if you create something special, you will be worth so much more in the long run.

Fourth, innovate and take some carefully considered risk. Accidents will happen, but accept that, learn from them, don't do it again and grow.

Finally, please remember that what you do is very important and can be extremely rewarding. Do not turn it into a window dressing exercise; strive to make a difference at some level.

Oh, and have fun — this is actually a very interesting field. 



Hue Dang

ACAMS Today: Describe your current position and responsibilities

Hue Dang: I am the Regional Head and Director of Asia Pacific for ACAMS. Part

of my role is to support ACAMS' mission of promoting sound AML practices and procedures and fostering growth of the AML community within the country and regionally by building relationships with Asian financial institutions, law enforcement agencies, and regulators. In addition, my team and I are equally focused on building the membership base and to further enhance the recognition of the CAMS certification program as the standard for assessing AML knowledge and experience with its emphasis on being a practitioner's focused exam.

AT: How did you become involved with ACAMS and why?

HD: I worked as a Bank Examiner with the Federal Reserve Bank of Boston for a number of years before moving to Asia more than 10 years ago to become an investment banker with Barclays and Citibank in Singapore, then as Director of Business Development at Thomson Financial in Hong Kong.

ACAMS was growing in the Asia/Pacific region and Ted Weissberg, the ACAMS CEO, whom I had worked with at Thomson offered me the opportunity to be the



Regional Head and Director of Asia Pacific. It was a perfect fit given ACAMS' role as an independent third-party situated between regulators and private-sector industry practitioners. Also, my background as a former regulator, coupled with private-sector experience in investment banking, enabled me to establish dialogue with both such seemingly divergent parties with greater ease. In essence, I could “talk-the-talk” and “walk-the-walk” with the regulators and the industry practitioners and I am able to understand their viewpoints.

I am very excited for this opportunity to lead ACAMS in helping governments and financial institutions in Asia in their fight against money laundering and terrorist financing through the promotion of AML education and training. ACAMS is in the unique position of being able to facilitate and foster the AML community and can play a key role in providing leadership. I am honored to have this opportunity to play such a seminal role in the growth and development of ACAMS in Asia, as well as AML community in this region.

AT: What developments have occurred in Asia since the opening of the ACAMS Hong Kong office?

HD: As is standard in most country's AML legislative framework, AML education and training is a requirement for all

financial services professionals. The challenge is defining the criteria to be used to establish the curriculum necessary to meet this AML training requirement. Our approach with each country in meeting our mission to promote AML education and training is to identify the key stakeholders who provide training to the financial services industry. We have signed a number of partnerships in this regard.


The first partnership we signed was with the China Center for AML Studies of Fudan University in Shanghai in May 2009. This partnership has the support of the People's Bank of China, and was a transformational event for ACAMS in Asia. One of the first steps in this partnership was the translation of the CAMS certification program materials into Chinese by Fudan University, to facilitate the growing interest in ACAMS' certification program by having the materials available in Chinese. Organizing the 2nd Annual AML/CTF Conference Asia Pacific, co-organized with Fudan is another step in us cementing our partnership with Fudan University.

Our second partnership was signed with New Finance Society Institute (NFSI) in Seoul, Korea, whose Founder and Chairman was a former head of Korea FIU. NFSI and ACAMS will work to promote the ACAMS certification program to compliance officers in Korea.

Our most recent partnership was signed with the Taiwan Academy of Banking & Finance, and the Bankers' Association, and the AML Research Center at National Chin-yi University of Technology, with the overall goal of promoting AML training in Taiwan — including the ACAMS certification program. Our first effort in promoting the 1st Annual AML Seminar for Taiwan, held on 27 January 2010. The number of attendees greatly exceeded our expectations at 180.

One partnership that will be signed in February or March 2010 is with the Institute of Financial Services, the training arm of the Monetary Authority of Macao for the financial services industry.

AT: What is your vision for ACAMS in Asia?

HD: It is my vision that ACAMS' AML training and certification programs become the standard by which prospective employers will point to a candidate interested in the AML field to demonstrate his or her commitment in this area by either having been CAMS-certified or by enrolling in the ACAMS certification program. It is also part of my vision that the compliance community in Asia will look to ACAMS to provide and facilitate the training of the latest AML trends and practices to industry practitioners. 

SARCSnSTRIPS™



Produced by ComplianceComm

[Know who you're doing business with.™]



Let Regulatory DataCorp™ (RDC™) help.

Is she a client? A vendor? A contractor? A key employee? *Is she a legal, reputational or financial risk to your firm?* Your job is to know before it's too late. Our job is to help.

We are Regulatory DataCorp (RDC), the most trusted source for enhanced due diligence among the world's leading financial institutions. RDC was founded in 2002 by 20 global financial services industry leaders. Today more than 6,600 users rely on RDC to ensure compliance with KYC, AML, FCPA and other regulations.

Why? The most comprehensive risk-related database ever assembled:

- Five million risk-relevant events
- 4,000 new records added daily
- 15,000 global sources

And the most responsive, flexible risk-related database ever assembled:

- 42 risk categories: monitor only risks relevant to your institution
- Pick up criminal or terrorist activity by group or individual
- Ongoing monitoring
- Delivery options that suit your needs and budget

Know who you're doing business with.™ Let RDC help.



RDC

Regulatory DataCorp

Know who you're doing business with.™

+1.302.353.5700

Solutions@RDC.com

www.RDC.com

The Nexus between financial crime, money laundering and terrorist financing

Raj Rajaratnam, is the founder of the large technology hedge fund, Galleon. According to *Forbes Magazine*, he ranked as the world's 559th richest person with a net worth of US \$1.3 billion, and is one of Sri Lanka's most successful entrepreneurs. He reportedly came under scrutiny during a federal probe into the Tamil Rehabilitation Organization (TRO), a charity, which was charged with funnelling large funds to the Sri Lankan terrorist organisation, the Liberation Tigers of Tamil Eelam (also known as Tamil Tigers or LTTE)¹.

In October 2009, Raj Rajaratnam was arrested and accused of earning some US \$20 million from stock trades, based on insider information provided by corporate executives. The SEC filed parallel civil lawsuits² against him and more than 20 other hedge fund executives and corporate insiders. The US media reports referred to the Galleon case as the country's largest hedge fund insider trading case³ (see also SEC Chart⁴).

The Federal prosecutors in New York have charged Rajaratnam with securities fraud and conspiracy to commit securities fraud. In December 2009, Rajaratnam was indicted for securities fraud and conspiracy. He pleaded not guilty and requested that the court reduce his bail to US \$20 million. The *Wall Street Journal* reported

– The Raj Rajaratnam case

¹The Liberation Tigers of Tamil Eelam ("LTTE") are considered a terrorist organisation by Sri Lanka, the United States and the European Union. After decades of civil war, the government declared victory over the LTTE in May.

²See SEC website for further details: <http://www.sec.gov/litigation/litreleases/2009/lr21255.htm>

³See following link for graphical representation of the allegations as reported in the Wall Street Journal http://online.wsj.com/article/SB126204917965408363.html?mod=WSJ_hpp_sections_tech-project=GALLEONWEB3%26articleTabs=interactive

⁴<http://www.sec.gov/news/press/2009/2009-235-chart.pdf>

on 6 January that his request was rejected and that federal prosecutors had instead planned to file additional insider trading charges against him, as evidence had been uncovered suggesting that he had already started his illegal activities in 2004 rather than in 2007 as previously believed. Based on this additional evidence, the prosecutors reportedly estimated that Galleon had generated at least US \$36 million in illegal profits rather than the original estimate of US \$17 million when the case was first reported in October 2009.

Investments in Sri Lanka and allegations of terrorist financing

The *Financial Times* reported that Rajaratnam returned to his country of birth, Sri Lanka, in 2002 after the declaration of a ceasefire in the civil war and began investing in the stock market. One of his first investments was in Hayleys, a leading Sri Lankan producer of rubber gloves. When the insider trading case emerged in the US, Rajaratnam allegedly held US \$100 million in Sri Lankan stocks, including nearly 10 per cent of the country's biggest listed company, John Keells Holdings. His New York brusqueness reportedly got him into trouble in a country increasingly polarized between the dominant Sinhalese Buddhist community and the Hindu Tamil minority. This conflict was made worse by the terrorist financing claims.

Interestingly, Rajaratnam was also investigated in Sri Lanka. The investigations are linked to donations he, among several wealthy overseas Sri Lankans, made to the TRO following the Tsunami in 2004. The TRO is thought to have been a front organization for the LTTE. The US Treasury Department froze TRO's assets in November 2007 because of alleged links to LTTE.


The *Financial Times* reported that after the 2004 Tsunami, Rajaratnam provided relief funds to projects for each of the island's ethnic groups, Tamils and Muslims, as well as Sinhalese. He also gave millions of dollars to the TRO, which two years later was found by the US to be funding LTTE.

According to ABC News, the TRO received more than US \$3.5 million from Rajaratnam. The Sri Lankan Central Bank reportedly said that it is still probing him, and a Sri Lankan military spokesman has warned he would be arrested if he returned. Other sources claim that the Sri Lankan central bank investigations found Rajaratnam to be innocent based on the fact that the TRO had not been banned by the Sri Lankan or US government when Rajaratnam made the donations. Rajaratnam and his father have also been named in a civil lawsuit in the US alleging they supported LTTE. A case in the US District Court in Brooklyn reportedly identified Rajaratnam's name in connection with funds funnelled to LTTE through a fake charity. His lawyer has rejected the allegations and denied that his client supports LTTE.

Risk-based approach required – the need for adequate enhanced due diligence and political risk assessment

Whether Rajaratnam knowingly funded LTTE or not, the Galleon case is another good example of how sophisticated financial crime, money laundering and terrorist financing activities can be inextricably linked.

This case highlights the money laundering and terrorist financing risks faced by investors and financial institutions, and underlines the importance attached to conducting enhanced client due diligence. Equally important is including an appropriate political risk assessment in order to effectively manage and mitigate the risks attached to non-governmental organization (NGO) and other charitable organizations, as well as their associations and activities, particularly those located in high-risk jurisdictions.

Although it is always important to look for what is not there and to try to understand why information is either lacking or illogical, the Galleon case, like many other recent Ponzi schemes which have surfaced the question of whether a client and or business is "too good to be true?" equally needs to be at the focus of AML research and enquires. 

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

Too good to be true?

Hedge fund AML risk, due diligence,
potential fraud and misbehavior



There are few investment vehicles with less transparency than hedge funds. Lack of transparency, limited regulation and increased access to these funds by the general public create significant opportunities for insider trading as well as pure fraud.

The Madoff scandal opened the floodgates on identification of hedge fund fraud as poor market conditions and fear of fraud caused investors to seek redemptions and regulators to investigate — where they had access to affiliated parties. As 2009 closed with continuing coverage of the Galleon scandal, the most massive insider trading fraud discovered to date, 2010 opened with an article from the Associated Press reporting that Ponzi schemes were up almost 400 percent in 2009. There is no question that the last two years have taken the lid off of Pandora's Box on hedge fund fraud and misbehavior.

In the case of Ponzi schemes, most victims were referred to a fund by a trusted financial advisor, a friend with community ties or a family member. Many of these schemes survived years without detection. We all want to believe that family, friends and colleagues have our best interests at heart and that they are honest, upstanding citizens. Unfortunately, it's not always the case.

Firms that deal with large hedge funds and/or high net worth clients will complete significant due diligence prior to introducing their clients to a hedge fund, taking a hedge fund on as a client or placing firm funds with a hedge fund. However, small funds may fall outside of these procedures because they have not disclosed their activities to the broker dealer or bank housing their account or they are self-custodying assets. Anti-money laundering (AML) professionals can focus on key elements of typical due diligence to assist in early identification of potential issues.

Firm due diligence

Due diligence by the alternative assets group or a credit and risk function at a large firm is likely to focus on the background of the fund's managing partners, the legitimacy and track record of the investment strategy and the perceived risk to invested capital. To do this, an analyst will gather general information about the fund and its partners, as well as regulatory and legal history, performance of various funds under the groups control, specific funds offered and subscription documents, information about key personnel, valuation methods, operational details such

as number of trades and prime brokers, names of service providers and make-up of investors in the fund, etc. Firms that complete this level of due diligence generally integrate AML needs into their processes.

Significant exposure exists for firms that service smaller hedge funds and, due to the nature of their systems or processes do not identify and evaluate the risk of those funds. A small fund operating entirely in the retail space may show patterns such as regular round dollar deposits (subscriptions) by check or wire from multiple sources, wires to issuers and delivery of shares from said issuer and withdrawals (redemptions).

If an account is suspected of operating as an investment fund and has not been subjected to enhanced due diligence, requests for offering, subscription and partnership documents related to the fund are appropriate. If the client denies acting as a fund and/or refuses to cooperate, immediate escalation to business line management is appropriate. If the suspected fund cooperates, enhanced due diligence should be completed on the key personnel including managing partners and authorized signers.

Information gathered by the alternative asset or credit and risk department analysis may be copied and organized into the categories below. The focus of the review is not the legitimacy of the investment, but inconsistencies in information, gaps in expected controls and/or negative regulatory or legal history of key individuals and/or entities.

Fund details and strategy

- The name of the fund and its details including address, management company or managing partner, organization chart and key contacts
- Fund marketing materials
- The prospectus or offering memorandum, subscription documents and partnership or operating agreements
- Audited Financials
- Key Personnel

Service providers with key contact name, phone and address for each

- Administrators (Offshore and Onshore)
- Lawyers (domestic/international)
- Auditors
- Prime Brokers/Custodian
- Executing Brokers
- Marketers/Capital Introduction Services

Operational details and controls

- Who supervises daily trading at the firm?
- How many executing brokers are used?
- Who has the authority to direct money or asset movements? Confirm they are included in the list of key personnel.
- How are securities valued? If an outside firm is used, confirm they are listed in the service providers.
- Does the fund have a policy on conflicts of interest, a compliance manual and a code of ethics?
- Does the fund management company share common space with another financial services company? If so, gather information on the company and its relationship to the fund.
- How is viability of individual investments determined? Does the fund require audited financials for investments that it makes?

Areas of focus

Focus on key control points such as custody of the assets, suitability and legitimacy of service providers, affiliations between the fund, service providers and underlying investments, as well as the profile of investors. This should provide enough information to establish whether the activity is potentially suspicious and/or requires closer review.



AML CHALLENGES

Enhanced due diligence, which includes legal, regulatory and reputational risk, should be completed on all key personnel and service providers. Any negative findings should be evaluated in the context of the party's ability to influence trading or access to the assets invested.

Custody of the assets

In real estate, the selling agent's mantra for success is location-location-location. When dealing with the protection of assets from pure fraud, it's custody – custody – custody. A reputable third party custodian audited by an independent accounting firm ensures that the assets you place in the manager's hands are subject to an independent set of controls.

Funds which have close relationships with their service providers (e.g., under common or significantly similar control) can be higher risk. Common addresses, ownership, signatories or controlling parties should be noted and researched. Questions should be asked regarding the relationship between financial services companies sharing the same address.

Suitability and legitimacy of service providers

Any accounting firm that you rely on should be registered with the Public Company Accounting Oversight Board ("PCAOB"). This ensures that the auditor is qualified and subject to regular review and inspection to confirm that it complies with accounting standards. Inspection reports available on the PCAOB website detail how many offices, partners and professional staff a firm has. This information can be used to form a general opinion of the adequacy of the accounting firm's resources.

Shortly after the Madoff scandal broke, it was disclosed that the accounting firm for his funds was controlled by a single accountant who was occasionally seen in his small office.

While this information was gathered from review of PCAOB records, CPA registration, interviews and physical inspection of the CPA office, you can form some opinions from the comparison of inspections over

time. For example, on August 27, 2009, the Securities and Exchange Commission lodged a complaint against Michael Moore & Associates ("Moore") alleging that the firm issued false audit reports prepared by unqualified staff that failed to comply with PCAOB standards. The complaint alleged that Moore issued audit reports on 300 clients, most of which were shells or companies with limited operations trading on the pink sheets.

A review of the inspection reports available at www.pcaobus.org shows that Moore was inspected in 2005 and again in 2007. In 2005, the inspection report shows one office with a single partner covering 3 issuer clients. In 2007, the inspection shows one office with two partners and six professional staff covering 162 issuer clients. The exponential growth in clients in the absence of growth in offices and additional staffing should be considered a red flag. If further research identified the same lawyers and/or other service providers serving the same clients as Moore, additional investigation into those individuals should be conducted.

Third-party marketers or parties providing capital introduction services should be registered with a broker dealer. These individuals can be evaluated by reviewing U4/U5 data available from the brokercheck tool at FINRA. See www.finra.org.

Affiliated entities


Affiliation between the custodian and the money manager can be cause for concern.

Like Bernie Madoff, Paul Greenwood and Stephen Walsh controlled the broker dealer where their hedge funds were housed. Allegedly, Greenwood and Walsh, through Westridge Capital Management and WG Trading LLC bilked investors of approximately \$550 million between 1996 and early 2009 when a National Futures Association ("NFA") audit identified that \$794 million of the \$812 million identified as assets of the funds were personal promissory notes from the pair.

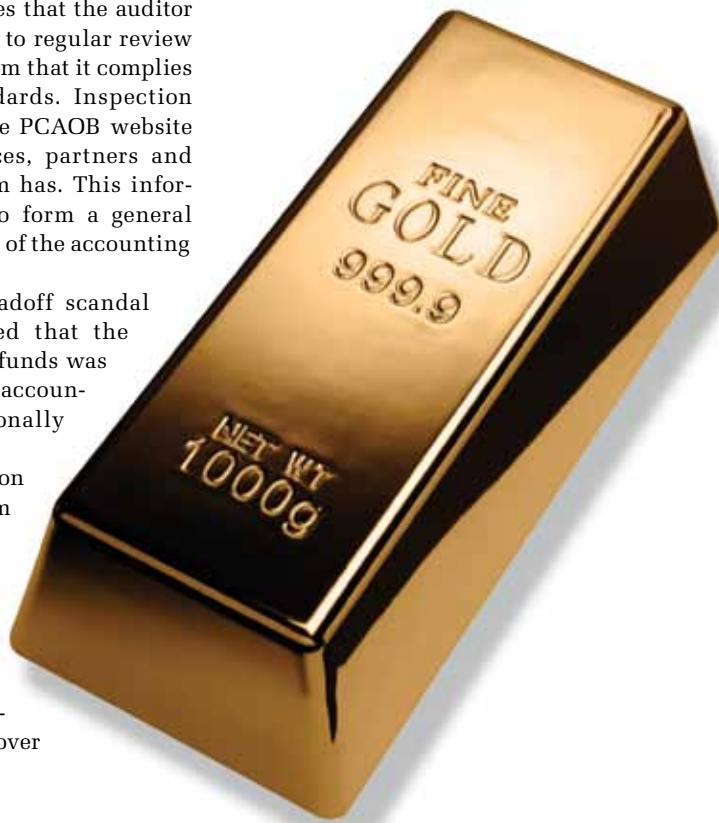
Service providers with clean records should also be investigated to determine if there are undisclosed associations to the entities that they service or to parties with close relationships to the entities that they service.

Quality and legitimacy of the investments

Hedge fund strategies are varied and complex. The AML function is not typically responsible for evaluating the legitimacy of an investment strategy and doing so may introduce inappropriate risk to the firm. Policies and procedures should exist for referring suspected investment funds to the appropriate credit and risk committee.

The AML function may review offering memorandum or prospectus in some situations. For example, when an account believed to be held by an investment fund has significant activity in low priced securities, the offering memorandum may identify if such investments are valid. Explicit inclusion or exclusion of such securities will allow the AML function to close or escalate an investigation. Additionally, the offering memorandum will disclose whether the shares are legally restricted and/or if there are limitations on sale or transfer. An assessment of the transferability of shares should be made by the group responsible for lifting restrictions on shares. The SEC has focused on identifying and litigating unregistered distributions over the past couple years. Careful evaluation of the circumstances of the sale is necessary to avoid charges of facilitating the sale of unregistered securities. 

Aaron Fox, managing director, IPSA International Inc, Minneapolis, MN, USA, aaron.fox@ipsaintl.com





A single alert speaks volumes.

Maximise your payments screening program by minimizing false alerts with Dow Jones

Dow Jones Sanction Alert

The call for increased transparency in international payments has been answered with new NACHA rules and changes to SWIFT message formats. Businesses that do not significantly change their payment screening process today will be buried in alerts, mostly false.

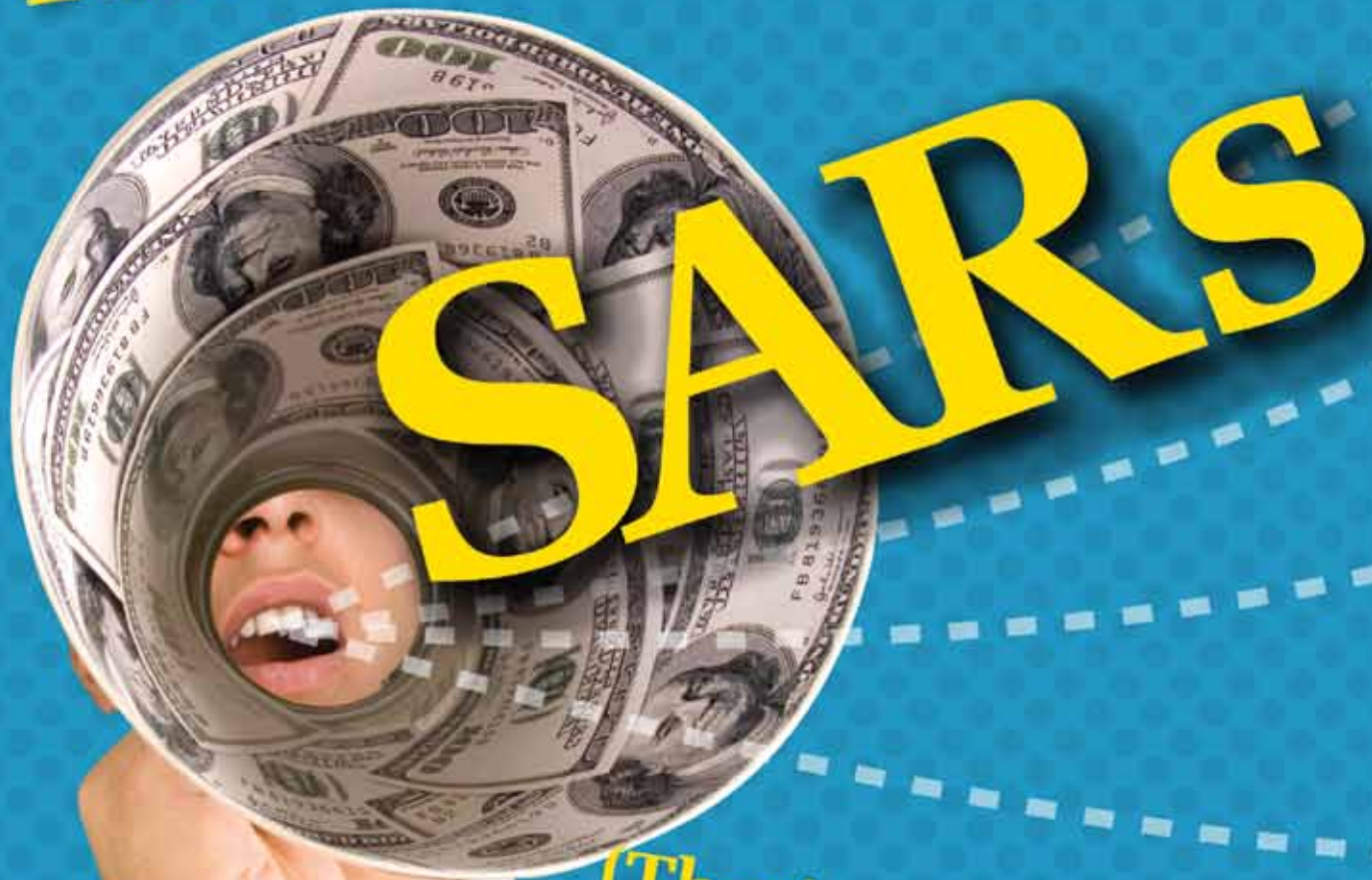
With custom risk settings, a unique consolidation platform, and sanctions data optimised for new international payments regulations, Dow Jones Sanction Alert effectively minimises the number of false alerts without increasing exposure to risk. This dramatically reduces compliance professionals' workload, minimising the risk of human error and

delayed payments, enabling firms to avoid the financial and reputational damage caused by a potential sanctions breach.

For more than 140 years, Dow Jones has been the source for trusted, authoritative business information. Today, over 1000 financial institutions rely on Dow Jones Risk & Compliance globally for mission critical compliance data.

To learn more about Dow Jones Sanction Alert, call +1.800.369.0166 (U.S.), +44.203.217.5100 (Europe) or +61.2.8272.4600 (Australia and Asia) or email riskandcompliance@dowjones.com.

The trouble with



(They're nothing special)

Despite the many and varied perceptions about suspicious activity reports (SARs), they were designed simply to be the financial community's confidential informants for law enforcement. Much of the rest of the Bank Secrecy Act (BSA) can be summed up as a way to provide investigators with a paper trail for that very elusive item — currency. The trouble with SARs and BSA in general is that rarely can anything special be denoted about currency.

Law enforcement on the other hand is all about specialties. On the Federal side, “Special Agents” have jurisdictional limits on the particular sections of the United States Codes they are sworn to enforce. DEA specializes in drugs, ATF in guns, IRS in taxes and the FBI having numerous, but not unlimited specialties. Even state and local agencies have specialized units to cover particular types of investigations or functions.

Unfortunately, SARs quite often report activity that cannot be sorted into these specialized compartments. Until BSA enforcement becomes a more recognized specialty onto itself, many valuable SAR leads will continue to end up in the waste basket. Money laundering too often has played a secondary or back seat role to enforcement, but when SARs thrust it up front, many investigators become uncomfortable with this primary role.

For example, a business owner is approached by a semi-regular customer. The customer claims to own a “consulting” business nearby. They are intentionally mysterious and there are neighborhood rumors speculating what they really do. They've been a good customer with a “keep the change” attitude. The customer says they are having trouble with the tax man and asks for a favor. They produce an envelope with a large stack of cash and asks that this business owner merely write them a check in a couple days for all, but the several hundred dollars of it they are willing to pay for this favor. If the offer is accepted the envelopes will be dropped off regularly.

Scenarios similar to this play out daily, thousands of times in communities all across the country, with cash-centric businesses being the primary target. For the owners who accept this type of offer, anomalies in cash deposits will soon follow. This owner may structure the cash deposits, and quite often will also separate this cash from regular or legitimate business deposits. This type of anomaly will more often than not

be noticed by the financial institution and a SAR will be filed. It sounds like a cut and dry money laundering scheme but step back and analyze just what is being reported and what an investigator reviewing the SAR has to go on.

Run every investigative database available on these business owners and you will find nothing to reflect anything illicit. Conduct weeks of intense surveillance and you will never observe criminal activity at these businesses. At best the owner may strongly suspect what illicit activity this customer's money is from, but will rarely have any firsthand observations of that. Willful blindness serves both parties well here. The real problem is to get an investigator to take a look in the first place. Is the customer a drug dealer, bookie or pimp? None of these enforcement specialties will show interest without some nexus to the “specified unlawful activity” that is the source of the cash. The SAR writer or financial institution can provide nothing to help. This owner is the only one who “may” know, but in this catch 22 no agency will initiate an investigation without that nexus.

Structuring is a felony by itself, but there has been a nagging tendency to view it as an excusable or “accidental felony.” Somehow aggressive enforcement is perceived as more likely to entrap Grandma in the act of finally depositing her previously secreted savings than to expose these schemes. A more “totality” approach to these cases will quickly reflect that structuring is far from an “accidental” crime. Structuring paves the way for fraud, crime and schemes that are less than noble.


Those who acquire bulk currency as a regular legitimate business function have found it necessary to develop systems and procedures to account for the inherent risks. The acquisition of bulk currency outside this world rarely has legitimate motivations. It is difficult to craft a scenario in which bulk currency is required, or is a prudent business practice. Even a few structured deposits quickly add up to quantities of currency law enforcement would be negligent to ignore. Any marginally competent investigator can easily sort Grandma out of the mix. To make this work however, BSA violations need to be as much a primary specialty for law enforcement as it is within the financial community.

Look into a number of cases that have dominated headlines of late and you will likely find there were many “little mistakes” that were ignored far earlier

than when the larger scandal unfolded. SARs are the neighborhood watch of the financial community. In the real world, law enforcement shows up when a suspicious person is reported. They need to show up more for the same reason in the financial world.

“If you can't investigate everything you can't investigate anything!” This is an often repeated point that instructors make to their detectives-in-training. The principles of investigation do not change from simple assault to homicide. Although a DEA Agent may specialize in drug trafficking, most are very capable of following leads in many other specialties. The same holds true for any respectable federal, state, or local investigator. The problem is that there are some real jurisdictional issues and many managerial ones for investigators to continue working cases without a way to articulate a nexus to their specialties.

Even when confronted by law enforcement, these business owners are not likely to initially confess to the money laundering scheme. In general, people will admit to the lowest level of culpability they believe will be accepted. Many drunk driving convictions were predicated on the driver's self admission to consuming “two beers.” Underreported income, unpaid taxes, and cash hoards are just a few of the “two beer” excuses in the money laundering world. Many of these investigative targets are sympathetic figures who have established legitimate business credentials. It generally takes a very skilled investigator to get beyond that. Most often the investigator is engaged in a “semi-bluff” in not accepting the excuse put forward. These backroom deals are more often suspected than ever fully exposed.

The “flip-side” here is that any intervention by law enforcement will likely dismantle this scheme. Both the business owner and nefarious customer will be leery of each other following any overt investigative contact. “Placement, layering and integration,” have real world meanings but a difficult, not insurmountable application within law enforcement. 

Steve Gurdak, CAMS, Alexandria Virginia Police Detective and currently the Group Supervisor of “Operation Financial Compliance, a Money Laundering Task Force under the Washington/Baltimore HIDTA (High Intensity Drug Trafficking Area), Alexandria, VA, USA, sgurdak@va.wb.hidta.org

Climate change and the risk of money laundering



As environmentalists, politicians and corporations negotiate for suitable international agreements to address climate change, one method has gained considerable favor. The “cap and trade” method allows for the purchase or exchange of carbon or emission credits. Under the system, incentives are given for the reduction of greenhouse gas emissions by allocating carbon pollution allowances to member states to fulfill their respective obligations under the U.N.’s Kyoto Protocol.

Companies that emit less than their allowance can sell the difference on

the trading market to firms that exceed their established limits. The European Union has already implemented such a program, and more recently, the United States has embarked on establishing a similar program.

The program’s overall objective is to create a market for the conservation of energy and reduce carbon and other emissions. When fully implemented, such markets are likely to involve considerable sums of funds being transferred from those that are buying such credits to those that are selling. Because the programs will create a mechanism for the transfer

of such wealth, it is vulnerable to money laundering and other financial abuse. Therefore, measures should be taken to prevent exploitation of these programs by organized crime and money launderers. Already, in a recent investigation by European law enforcement officials, evidence was uncovered suggesting that Europe’s carbon trading scheme was being used by some organized criminal groups to steal and launder some US \$7.4 billion (over 5 billion Euros) — money originally intended to help the environment.

In its statement released in early December from its headquarters in the


European Climate Exchange (London, UK), Nordic Power Exchange (Oslo, Norway), European Energy Exchange (Leipzig, Germany), Energy Exchange Austria (Graz, Austria), Climex (Amsterdam, the Netherlands) and BlueNext (Paris, France), as well as various other market platforms such as SENDECO2, Italian Power Exchange GME and Greenmarket, set up by Deutsche Bank at the Munich exchange.

Since its inception, more than 2 billion EUAs have been allocated to 12,000 emitting facilities in the 27 MS. Each transfer of EUAs is recorded in a national registry before it is centrally stored in the Community Independent Transaction Log (CITL) at the EU Commission.

The EU carbon market is estimated to be worth about €0 billion a year. The transfer of greenhouse gas emission allowances is considered to be a taxable supply of services, and thus these transactions can generate a considerable revenue stream for Member States. Unfortunately, just as in the case of other taxes, criminals have found ways to “beat the system.” Known as Missing Trader Intra-Community fraud (MTIC), organized crime groups have found a way to steal the revenue from these credits much in the same way as those methods identified in schemes involving the theft of Value Added Tax (VAT) credits, otherwise known as VAT carousel fraud.

According to the investigative report by EUROPOL officials, such fraud was accomplished by traders opening an account in a national carbon registry and then purchasing emission allowances without value added taxes from other companies in other countries. Those allowances were then transferred to the country where they were registered before the accused trader moved them to an unregulated broker, selling the allowances on a trading exchange, often through various buffer companies. Finally, the accused trader charged the value added tax on the transaction but did not submit that money to authorities.

Evidence of such suspicious trading activities were first noted in late 2008, when several market platforms saw an unprecedented increase in the trading volume of EUAs. Market volume appeared to peak in May 2009, with several hundred million EUAs traded. At that time the market price of 1 EUA, which equals 1 ton



Netherlands, EUROPOL stated that the European Union Emission Trading System, which was begun in 2005, had been the victim of organized crime during the past 18 months. The director of EUROPOL, Rob Wainwright, suggested that up to 90 percent of the market volume in some countries could have been caused by fraudulent activities. Mr. Wainwright went on to express his concern that such criminal activities would endanger the credibility of the European Union Emission Trading System and lead to the loss of significant tax revenue for the governments who were victimized.

The EU program sets a goal of limiting global warming to 2 degrees Celsius above pre-industrial levels in an effort to help reduce climate change and satisfy international obligations under the Kyoto Protocol. Each Member State assigns emitting facilities within its borders a certain amount of emission rights by means of a National Allocation Plan. These rights are known as European Unit Allowances (EUAs).

These emission rights are then made available for trading just like any other commodity on the market. In Europe, there are six trading platforms available:

AML CHALLENGES

of carbon dioxide, was around EUR 12.5. This resulted in losses of approximately 5 billion euros among the several national tax revenues involved.

France, one of the countries affected, has launched a criminal probe into four men who allegedly took part in the scheme, two of whom have already been jailed. According to a statement issued by French law enforcement authorities, the fraudsters used a device which allowed them, using specially created structures and screen companies, to collect value-added tax payments, without transferring them to the French Treasury, by buying carbon rights duty-free from overseas brokers and re-selling them at a price that included the French tax.

U.K. customs officials arrested seven people in August as part of an investigation into an alleged 38 million-pound (\$62 million) tax fraud related to carbon credits trading. The probe is ongoing according to a Revenue and Customs department spokesman.

To prevent further losses, several countries, including France, the Netherlands, the United Kingdom and Spain, have all changed their taxation rules on these transactions. France ended its value-added tax on trades of European Union carbon dioxide allowances in June, deciding to lift the levy because of the risk of carousel fraud. The U.K. followed in July, and the Netherlands has shifted the levy to the buyer. As a result of these countermeasures, the market volume in the aforementioned countries dropped as much as 90 percent.

EUROPOL, with the support of several Member States, has established a program to collect and analyze information in an effort to identify and disrupt the organized criminal forces behind these fraud schemes. Some officials fear that these fraudsters might soon migrate toward the gas and electricity branches of the energy sector.


Concerns that similar fraudulent schemes could occur under a United States-sponsored program have been raised by some policy makers. At least one case has already made its way to the courts. During the 1990s, a California program called the Regional Clean Air Incentives Market (RECLAIM) created a similar trading regime for “pollution credits” within its borders. One company, Automated Credit Exchange (ACE), provided a market for companies to buy and sell these credits. One of the owners of ACE, Ms. Anne Sholtz, was uniquely positioned to profit



from the market since she had previously been one of the co-creators of RECLAIM.

Evidence indicated that Ms. Sholtz’s knowledge of trading pollution credits helped bilk a New York-based company that traded in energy credits. That firm, AG Clean Air, bought \$12.5 million worth of her credits after Sholtz told the company that Mobil Corp. would need them for use at a Southern California refinery. Ms. Sholtz sent counterfeit faxes and e-mails to AG Clean Air that purported to document non-existent negotiations between her and Mobil, including a purchase and sale agreement with a phony signature. The scheme ran from 1999 to 2001, going undetected by the EPA. It finally began to unravel only after a local air quality board started getting complaints from companies that had dealt with Ms. Sholtz. A year later, her firm closed and went into bankruptcy. Two years later, she was arrested by federal agents. In 2005, Sholtz pleaded guilty before Federal District Court to wire fraud for using counterfeit documents and fraudulent pollution credits to pocket more than \$12 million and was sentenced to one year of house arrest.

It is clear that some sort of carbon trading or compensation program will be a key element of addressing global climate change and carbon emissions. Most policy leaders, as well as industry, have indicated a preference for a market-based system. Nevertheless, because a market-based

approach opens the possibility for money laundering, fraud and other abuse, steps should be implemented to identify and prevent such activities. Some legislators have begun to recognize this possibility and have called for any enabling legislation to include provisions for oversight, monitoring and enforcement where abuse is suspected. At least one alternative has been proposed. Senator Maria Cantwell (D-Wash) has proposed a program similar to “cap and trade”, but which instead of providing funds to the private sector would revert any profits or “dividends” from the sale of carbon credits to the public at large, either through direct tax refunds or through public programs designed to counteract the adverse effects of pollution. Regardless of the final details of such approach, attention should be given to ensuring that the operation of carbon credits programs are based on actual efforts to reduce or reallocate carbon emissions, that any transaction which results in the transfer of wealth or assets under such programs are based upon true and verifiable criteria, and that the overall programs are insulated from the type of fraud and other abuse that would end up defeating the beneficial purpose for which such programs were intended. 

Kenneth E. Barden, CAMS, J.D., MFI Project, Ramallah, West Bank, kenneth_barden@yahoo.com

6th Annual ACAMS Anti-Money Laundering & Counter-Terrorism Financing Conference Europe

Hilton Amsterdam, The Netherlands

Pre-Conference Workshops **6 June 2010**

Main Conference **7-8 June 2010**

Adopting Regional Best Practices to Combat Global Threats

Comprehensive two-day programme provides critical AML/CTF updates:

- Understand the impact of Credit Suisse and UBS enforcement actions on your organisation
- Assess key milestones in Third EU Directive implementation
- Navigate complex PEP and economic sanctions requirements
- Prepare to comply with new tax evasion and anti-corruption regulations
- Stay ahead of the latest financial crime schemes

Media Partners:

The UBS case

Eileen Mayer, the former Chief of IRS-Criminal Investigation (CI), gave a very informative luncheon presentation to the US Capital Chapter of ACAMS on January 15, 2010. Michael Mancusi and Winston & Strawn hosted the presentation. Ross Delston, CAMS, GlobalAML.com, moderated.

Mayer discussed the following:

- The structure of CI, how it is organized and its major cases;
- CI's work on money laundering;
- How a typical case is investigated;
- The Swiss tax evasion cases; and
- How the economic meltdown has affected CI's work.

Mayer noted that more than 50 percent of CI's cases involved the proceeds of funds that were legally obtained; 35 percent involved the proceeds of funds illegally obtained; and approximately 12 percent involved narcotics, money laundering and terrorist financing.

Mayer recounted some of the background of the UBS case and noted that the IRS has expanded its presence in the Pacific Rim and that she expected additional cases involving similar facts. As a result, she said that it is useful to review the facts and circumstances of the UBS case.

UBS AG, the largest Swiss bank and one of the largest banks in the world, entered into a Deferred Prosecution Agreement and paid \$780,000,000 in fines, penalties, interest and restitution to the US in February 2009. The action against UBS was due to activity in its offshore wealth management business, which the U.S. Department of

Justice (DOJ) said constituted a conspiracy "to defraud the United States by impeding the Internal Revenue Service."

According to the criminal information, in 2000, after acquiring the U.S. brokerage firm Paine Webber, UBS entered into an agreement with the IRS whereby UBS was required to "report to the IRS income and other identifying information for its United States clients who held United States securities in a UBS account . . . [and] to withhold income taxes from United States clients . . ." According to the DOJ, not only did UBS fail to live up to the agreement, it knowingly evaded the requirements by helping U.S. taxpayers open new UBS accounts in the names of nominees and sham entities and transferring the assets of the original accounts into these newly created accounts.

While the UBS case has been viewed by many as strictly a tax evasion case, there are additional repercussions, including potential money laundering and the failure to file Reports of Foreign Bank and Financial Accounts (commonly known as FBARs). There are five different reasons for maintaining an unreported foreign bank account:

- Money laundering;
- Evasion of taxes;
- Hiding assets for illegitimate purposes other than tax evasion (e.g., avoiding legal or medical malpractice claims, avoiding alimony);
- Hiding assets; and
- Seeking political and/or financial stability.

In settling this case, UBS admitted wrongdoing, and agreed to "expeditiously exit the business of providing banking service to U.S. clients with undeclared accounts." More significantly, UBS further agreed to turn over the names of approximately 250 account holders that had surfaced during the course of the investigation to the U.S. Government.

As we know, the attention of the DOJ and the IRS has expanded beyond UBS to include other international banks with offshore wealth management business and to individual U.S. clients who set up offshore accounts in Switzerland and elsewhere and who failed to disclose the existence of the accounts or the assets or income associated with the accounts.

The seriousness of these cases involving cross-border wealth management business for illicit purposes is borne out by the

estimates that, according to an October 30, 2009 *Wall Street Journal* article, one third of private banking clients in Switzerland are non-residents and that tax evasion by non-residents could represent 25 percent of the Swiss private banking market. The same article, however, notes that the biggest banks, such as Credit Suisse Group, UBS, Julius Baer Group AG and Pictet & Cie, are taking steps to avoid doing business with potential tax evaders by focusing on and increasing onshore businesses in various countries. A further motivation of reducing and/or eliminating this business, of course, is to protect the bank from involvement in money laundering and tax evasion.

In keeping with the expanding focus on individuals, the day after the Deferred Prosecution Agreement, the DOJ commenced a civil action to obtain the names of 52,000 American UBS account holders. After months of legal and diplomatic wrangling, the two countries agreed that UBS would produce approximately 4,450 names of American account holders on a rolling basis and after additional reviews. At one point, these accounts held approximately \$18 billion. Along with this effort, the IRS declared a qualified amnesty program which received an unprecedented response of 14,700 people coming forward to belatedly admit to the existence of an ownership or control interest in previously undisclosed foreign accounts. Consequently, it is clear that U.S. prosecutors will be concentrating on a large number of accounts and the banks and individuals connected with these accounts.

The focus that includes individuals, as well as banks, is not limited to the account holders. A November 17, 2009 article in the *New York Times* reported that the DOJ and the IRS are looking not just at the direct account holders, but “are also looking at a web of financial advisors, lawyers, accountants and others who help the banks sell their services.” Thus, it is clear that banks, account holders and those who help them evade U.S. income taxes and the requirement to disclose the existence of foreign accounts will be the targets going forward.

In accordance with the agreement between the U.S. and Switzerland, UBS will be producing information on almost 4,500 American-held accounts that were in existence between 2001 and 2008, were unreported and had a balance greater than or equal to 1 million Swiss Francs (or approximately \$988,000). In addition, UBS will produce American-held

accounts that were in the name of secret offshore sham companies and had a balance of 1 million Swiss Francs. UBS will also produce American-held accounts that had a balance of more than 250,000 Swiss Francs (\$247,000) that involved “tax fraud or the like,” which is defined as including concealment of funds, the submission of incorrect or false documents to UBS or to the IRS and what the IRS terms “a scheme of lies.” The latter phrase would include the “use of false documents, related entities to repatriate funds in the offshore accounts, calling cards [referring to pre-paid phone cards] to disguise the source of trading, sham entities and debit or credit cards to repatriate funds for the payment of personal expenses.”

Last, UBS will produce information if the American account holder did not file a W-9 over three years since 1998 and the accounts generated annual income of at least 100 million Swiss Francs.

These criteria reduce the volume of potential accounts to a restricted number of relatively large accounts. Accordingly, the criteria perhaps explain how the original number of 52,000 accounts sought was reduced to approximately 4,500. However, it is clearly possible that future legal and/or diplomatic settlements whereby the bank at issue produces only a small fraction of what the U.S. prosecutorial authorities are seeking will become more and more infrequent.

In fact, Switzerland and other countries have embarked on a new tack of entering into international treaties that will make it easier to require banks to produce information about individual cross-border bank accounts. As the President of Switzerland has said, his country is willing to “expand existing cross-border cooperation within the framework of bilateral negotiations.” Already, Switzerland has entered into new treaties with France and the United Kingdom that will make it easier to pursue information on suspected tax evaders.

Another example of how the U.S. is proceeding against large banks with international clients is represented by the Citigroup settlement this past October. In that case, Citigroup was fined \$600,000 for allegedly assisting clients in avoiding taxes on dividends through a complex derivative scheme. According to an October 12, 2009 article in the *Financial Times*, the case “could herald a wider crackdown against Wall Street banks that used similar strategies.”


These cases involving the cross-border

wealth management activity of banks and their individual clients have dramatically increased the focus on tax evasion and the failure to properly disclose the existence of foreign accounts. Accordingly, banks, their clients and the professionals advising the banks and the individuals should take steps to ensure that:

- Proper monitoring systems and internal controls are in place for identifying potential misuse in cross-border accounts and transactions;
- Adequate and periodic training of staff and management is provided to guard against money laundering, tax evasion and other misuse in cross-border accounts and transactions;
- Adequate internal reviews and outside audits are conducted of cross-border accounts and transactions to identify weaknesses and gaps in this business;
- The purpose of cross-border accounts and transactions is legitimate and proper;
- Income placed into foreign accounts or generated by the accounts is properly reported; and
- FBARs are properly filed on a timely basis.

It is always better to self-disclose to the IRS and other authorities than to wait for them to uncover the activity at issue. Taking the chance that the activity will not be uncovered — because it involves too little money; because it is too well-hidden; or because the risk is worth the reward — is usually not a very good gamble. And the negative consequences for all of those involved can be immense.

At the time this article was being written, two Swiss courts ruled that the disclosure of the 4,450 accounts previously agreed to would violate the country’s secrecy laws, but, mysteriously, said that the production of the initial 250 names was fine. This leaves the IRS insisting on compliance and the Swiss Government in a quandary.

Do they overturn their own courts and decades of bank secrecy or do they allow the U.S. to resume its suit against UBS for the 52,000 accounts and, possibly, criminal action by the U.S. against the bank? The only thing the Swiss government is saying so far is that it is willing to negotiate. 

Robert S. Pasley, CAMS, AML and regulatory attorney, consultant, Alexandria, Virginia, USA, bob@pasleyconsulting.net

MONEY LAUNDERING THEN AND NOW

I have served in the anti-money laundering/financial crime field since 1983. Agreeing to write this article caused me to take a walk down memory lane. I clearly recall the first day I was asked by a very well-respected officer in the Royal Canadian Mounted Police (RCMP), former Assistant Commissioner Rod Stamler (now retired), to take an assignment within a newly named program, Anti-drug Profiteering. The mandate was simple: Ensure a comprehensive testing of Canada's existing laws, identify gaps in the system and develop a national training program which would provide the necessary tools for investigators to intercept proceeds derived from drug trafficking in order to thwart ongoing criminal activity.

At the outset there were very few countries that had developed programs we could study. The United States had a robust civil regime which was widely utilized by the Drug Enforcement Administration, but such an approach was not accepted within the political halls of Canada. Therefore an initial group of 14 keen investigators, which grew in 2004 to 19, became Canada's answer to detect proceeds of crime. As the individual assigned program responsibility, my job was to coordinate with all investigators, develop a management and investigative training program, liaise with international counterparts and coordinate with all other affected government departments.

Beginning in this new field was both challenging and frustrating. The entire financial industry was a total different creature relative to what we see today. Public and private working arrangements were essentially unheard of and the concept of stopping money laundering was seen as erosion on corporate profits and the security of client information. What must be realized, also at this time, experience was extremely limited with most investigators coming from the drug enforcement area as they had seen money laundering for years, but only focused on the drug product. This resulted in quick press releases where multi-pounds of drugs were rolled out for the cameras and investigators claimed success. The reality was drug traffickers kept getting richer and the drug

problem continued to grow unabated.

In the mid 80s through to the early 90s, money laundering was wide-open in Canada. It was not uncommon to see, while on surveillance, bags of money being carted into various financial institutions and be deposited without a question. Notwithstanding the openness of the system, the initial group of investigators forged ahead and was very successful in creating case law which resulted in proceeds of crime forfeited, even though freezing; seizing and forfeiture powers were non-existent. We saw judges creating legal precedent through their decisions, which, in many circumstances, challenged not only the Canadian Government, but governments

International acceptance

Throughout the 80s in Canada, the international community called on the RCMP to discuss how they perceived money laundering cases unfolding. What was very evident was that our approach was well ahead of what the political pulse was, and was being touted as being worthy of review by our foreign counterparts. Our early training was also considered ahead of its time, which resulted in extensive international travel providing training to our foreign counterparts.

RCMP approach was simple and the philosophy was that by providing the court with information pertaining to the lifestyle and spending habits of an accused, the presiding judge was able to appropriately take into consideration the level of the accused within the criminal hierarchy. Furthermore, it was argued that to minimize the rising level of criminal activity, it was necessary to minimize the motivating factor, which everyone accepted as being profit.

Co-operation and collaboration

RCMP also began a program in which there was recognition for the value of differing expertise. Units began using forensic accountants. Lawyers were engaged to help investigators maneuver through legal requirements pertaining to the obtaining of financial documents and there was an acknowledgement that all levels of law



— 25 PLUS YEARS IN THE INDUSTRY



enforcement needed to be seen as seamless investigative units.

During this same period, law enforcement and banks started to adopt very strong approaches toward each other; the banks claiming confidentiality of their clients and law enforcement claiming banks were the money laundering problem. This led to an interview (1986) with national media in which I blamed the banks for Canada's growing money laundering problem. Needless to say this garnered attention and served as the catalyst for several high level meetings in which the banking community agreed that we needed to work together to combat money laundering. However, they remained steadfast that their client privilege was sacrosanct. This ushered in a new era of opening the dialogue between law enforcement and banks.

As a result of the limited success of the program, and in response to international awareness of the destructive potential of money laundering, Canada began examining its legislative regime, as did many other countries, all of which committed to combat money laundering by becoming a signatory to the 1988 Vienna Convention.

Unfortunately due to the government process and despite the fact we had our first draft legislation in 1985, no viable legislation made its way to the table until 1989, and that was restricted to drug offenses. The impact through the 80s and early 90s was limited in scale and reality and dictated that a more comprehensive regime was needed to have a major impact on criminal organizations. The first workable legislation and commitment by the government to take money laundering seriously occurred in 1992. This holistic approach was one that was promoted as the only viable approach to combat the growing sophistication of organized crime.

1990s

In the early 90s Canada had still not expanded legislation to combat smuggling offenses and thus organized crime took advantage of this weakness. One organization, which became a high profile U.S. and Canadian target, was the Miller Organization which is believed to have laundered between \$600 and \$800 million

dollars between 1992 and 1996. It was this organization against which — in 1996, in partnership with our U.S. counterparts — we launched a successful undercover operation. The most disturbing aspect of this case is that one of Canada's pre-eminent financial institutions willingly accepted money from a correspondent bank in the U.S. with the full knowledge that it was derived from cigarette smuggling.

The result was that, once the issue was raised on the floor of the House of Commons, legislation was quickly passed (1997) to expand money laundering offenses to include smuggling. As for the undercover operation, we were successful in infiltrating the entire organization, resulting in the arrest of most members of the Miller organization and their supply lines. Additionally, evidence was obtained that aided Canada in its successful civil action against the cigarette industry.

This case highlights the fact that we needed a proscriptive regime in order to ensure all banks were providing intelligence on suspected money launderers. In the mid 80s the system was totally one of voluntary disclosure, which resulted in marginal success. Having had the opportunity to view disclosures held within one of the large bank's security departments, evidence demonstrated that the industry was still reluctant to provide information voluntarily, despite the fact that many reports submitted by branches were sufficient on their face to highlight possible money laundering activities.

At this time, international pressure was mounting and with the creation of groups such as Financial Action Task Force (FATF), Wolfsburg, Egmont Group etc, money laundering was being recognized as an issue that could only be effectively combated with wide-range cooperation. Banks throughout North America began to work with law enforcement while recognizing their corporate and community responsibility.

Banks became more collaborative and began recognizing that law enforcement had garnered a vast bank of expertise relative to money laundering throughout the previous decade. Banks that were proactive willingly opened their doors to have

law enforcement discuss money laundering red flags, along with how a public and private partnership was necessary if money laundering was to be controlled. Many of the large institutions started building their own infrastructure within Security Departments to help prevent their institutions from being used as vehicles for money laundering. Accounting firms accepted that forensic accounting was a new service offering that was required throughout the world and therefore, they made huge investments in personnel in order to be seen as being able to provide expertise to both public and private organizations.

Reality

What we failed to recognize early on was that the more sophisticated we became as a collaborative global community, organized crime became just as sophisticated. This sophistication was due to their capacity to have funds available to them that were on par, if not larger than government investments in technology and subject matter experts. Additionally, organized crime honed its skills as it learned the investigative techniques that were publicized during the numerous criminal cases being prosecuted whilst, unfortunately, law enforcement continued to maintain their generalist approach to resourcing, thereby failing to develop sophisticated white-collar investigators capable of attacking the largest criminal organizations.

Today

As a result of many early investigative successes and the firm commitment by many countries around the world to combat money laundering and associated organized crime activities, we are now dealing in a new era, one of sophistication and criminal partnerships which cross many borders.

I have raised alarm bells for the past several years arguing that we are falling behind the sophistication of many large criminal organizations. This failure is due to stretched budgets, onerous court requirements and a failure to develop the necessary expertise within the specialized units. It can be argued that the financial industry has, through proscriptive legislative requirements been required to invest millions of dollars in an effort to uncover money laundering and financial intelligence units have been established to analyze all of the financial flows but what begs to be asked, have enforcement

agencies around the world had the same required commitment and level of investment? Regardless of the country, the financial community would argue their efforts are now outpacing the capacity of law enforcement and that their level of expertise is growing at a faster rate than that of many law enforcement organizations due to their opting for skill development and remunerating based on this approach. In today's environment we are facing new realities and challenges. There is a massive increase in fraud offenses, ID theft, phishing schemes, intellectual property right crimes and cyber-crime, all of which require expertise. Drug trafficking has not abated, but the money laundering activities have had to become more sophisticated, relying on the incorporation of many companies to co-mingle the illicit revenue. The underground economy has become ripe for investment, as criminals can pay many of the trades, with cash. In turn, some small communities are seeing a revitalization of their downtown core through the influx of renovations which may be directly tied to criminal activities. In all cases, a front person with no criminal profile is seen as the Good Samaritan investor.

The current situation also requires law enforcement to conduct long and intensive investigations. With the current jurisprudence, cases that would have taken four investigators to bring to fruition a decade ago now can take upwards of 20 to 25. This has resulted in massive file backlogs and fewer and fewer cases seeing the light of day. Our financial communities complain that their commitment to combating money laundering and organized crime is far greater than what enforcement can muster and thus argue against further prescriptive measures.

When I first began my work in the money laundering field, I could not have imagined that I would be at the forefront of working within an international industry that has become a recognized profession. Those of us who were at the beginning could never have imagined that this industry would employ tens of thousands of committed people and become the focus of the world community. As we know, it is now a profession in and of itself: whether working in anti-money laundering compliance/intelligence and/or an AML investigative officer. The private industry has now embraced all AML requirements and continually seeks out subject-matter experts to help in the ongoing fight.

Drug trafficking has not abated, but the money laundering activities have had to become more sophisticated

Conclusion

Money laundering is no longer a foreign concept. The financial sector needs to continue to provide financial information to our respective financial intelligence units. These units need to embrace skill development and ensure they have a career stream for their personnel. Through the FIUs, improved data will continue to flow to law enforcement, which also must adjust and embrace skill development over the concept of Para-military rank regimes. They will need to consider skill-based pay in order to encourage the development of sustainable expertise. Our prosecutors also need to become specialized AML litigants. Through the creation of seamless teams with a common goal, we will have the requisite skills to combat even the most sophisticated organized crime groups; however, a failure to adjust will only serve to expand the power and reach of these same groups.

As organizations like ACAMS have demonstrated, a group of interested participants can work together and serve the world community in order to demonstrate a collective resolve to combat organized crime. To quote Edmund Burke, "All that is necessary for the triumph of evil is for good men to do nothing" For those of us who have been part of this industry for many years, we have worked to ensure those following us will have a base of knowledge from which to launch their careers and continue working with a goal to thwart organized crime's ability to move their illicit financial gains. ▲

Garry W.G. Clement, CFE, CAMS, AMLP, president and CEO, White-Collar Consultants and Investigative Group, City, Province, Canada, whitecollar@explornet.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?

Log onto www.ACAMS.org/Chapters



Australasian Chapter



NEW JERSEY AND YOU – PERFECTLY CORRUPT TOGETHER

Transparency International, a world-wide organization committed to exposing and fighting corruption, releases a yearly corruption perception index (CPI) report, which ranks countries in order of perceived corruption as viewed by businessmen and various independent sources both inside and outside each country. For 2009, the United States ranked 19th out of the 180 countries surveyed. You have to wonder how much better it could have been if the state of New Jersey was excluded. New Jersey has always been a hotbed for political corruption, but over the last several years the copious amount of arrests and indictments stemming

from that same corruption has made even the most cynical residents aghast at how widespread and blatant fraud and financial shenanigans have become. Influence peddling, bribery, tax evasion, self-dealing and outright extortion have become part of the everyday fabric of a state that has made the “Sopranos” television series seem subdued by comparison.

In July of 2009, the Federal Bureau of Investigation (FBI) arrested 44 individuals, including several mayors, assemblymen, lower ranking public officials and political sycophants, the charges ranging

from bribery to money laundering, with a shakedown or two along the way. The recent arrests crystallize a state where the government has continually been either unwilling, unable, or both, to police itself. After the arrests, Democratic Governor, Jon Corzine, the most unpopular man to ever be elected, gave a curious assessment of the situation. When asked if the arrests would hurt his reelection bid in November, since most of those arrested were Democrats, Corzine answered as only a politician



would, giving an ancillary answer to a primary question. He indicated, in essence, that the net result was that the system works because the perpetrators were arrested, adding that there have been hundreds of previous arrests over the years. That's analogous to saying we have two million people in prison for bad behavior, but not answering the fundamental question of why as a society we have so much bad behavior. Corzine's opponent in the race, Republican Christopher Christie, who made fighting corruption a central theme of his campaign, himself became embroiled in his own financial misadventure, surrounding the tax reporting of a loan he made to a subordinate.

The reasons

There is an abundance of reasons why corruption has become the state avocation. The first centers on population density. It's a simple fact of life that the more people you have packed into an area, the more potential for misconduct there will be. The second piggybacks off the first. New Jersey has multiple layers of government and public officials due to that same population density. New Jersey is also an expensive place to live and an expensive place to run for office. The salary for public officials pales in comparison to that of their contemporaries in the private sector.

Going hand in hand with the above is the lucrative construction and real estate development trade that abounds in northern New Jersey. This of course lends itself to government contracts, with those, especially on the local level, creating a breeding ground for the temptation to break the law. Anti-money laundering (AML) professionals are keenly aware of the high risks associated with the construction and real estate industry, but in the context of smaller cash activity, conventional wisdom speaks mostly to the possibility of workers, especially undocumented, being paid off the books. Bribery of lower level public officials, such as building inspectors, town council members, superintendents and mayors are equally commonplace. What makes the detection so difficult is the amounts, which generally range between \$1,000 and \$10,000. Unlike cash payments to employees, which are usually steady, a bribe is generally a one-time payment or a series of payments done on a random basis. A small structured cash deposit by a local official to his/her account (\$5,000 on consecutive days with no history of cash activity) could be a clear signal that the official has had their hand out.

Wheeling

While there is no comparison between making a campaign contribution and offering a bribe, in the eyes of many it still amounts to the same thing. Campaign contributions, however, are generally capped at specific amounts per election cycle, but a maneuver known as wheeling has generally made a mockery of New Jersey campaign finance laws — once again, predominantly at the local level. In a nutshell, wheeling is the structuring of campaign contributions by the establishment of political committees, allowing companies and individuals to easily exceed contribution limits to individual candidates by donating up to the maximum to each committee. The funds are then wheeled (transferred) into a main account and used on behalf of the candidates.

Despite the fact that even the most unsophisticated among us can see what's going on, those involved in wheeling seem to have the need to further try and disguise what they're doing. Many of the accounts are set up under the premise of obfuscating its purpose by using names that would lead one to believe it's nothing more than a small local fundraising committee, for example — Disabled Veterans Democratic/Republican Committee. What's even more offensive is that many times an individual who fits the particular class is used as a signer and quasi-front man. In many instances the political party name is left out for further obfuscation. Unfortunately, every now and then some well-meaning individual will make a small donation for what they perceive to be a worthy cause, not remotely aware that the final destination of their hard-earned money is a political campaign.

Wheeling is perfectly legal, but it goes right to the heart of subverting the integrity of government. When analyzing the contributions made to these political committees, you immediately realize that the bulk of the money is coming from companies that survive and flourish because of profitable government contracts from local municipalities. It's the quintessential quid pro quo, calling into question whether the taxpayer is getting their money's worth when no-bid contracts are awarded. Wheeling also raises the question of whether funds being wheeled are actually all from the one source — or is that source nothing but a front? When reviewing the deposits to political committees, look for multiple checks from companies that cannot be defined or have a post office box as their address. Additionally, pay

particular attention to the check signatory, which may reveal that several companies are under one person's control.


At the very least, reviewing and investigating political committee accounts can provide a wealth of information on the players, which may be beneficial in unmasking other interlocking relationships.

Smurfing

Practically impossible to discover without a break are individuals used as front men to make direct campaign contributions. Like bribery, it's difficult to detect because of the small amounts, usually between \$500 and \$1,500. The fact that all individuals involved may bank at different institutions also reduces detection of any common denominator. The standard modus operandi is that a big political donor, who either controls a workforce, or has friends who control a workforce, uses that workforce to funnel what appears to be individual campaign contributions, which when aggregated come to well in excess of the individual contribution limits. The political donor gives the workers cash, which they in turn deposit to their personal checking accounts. They then proceed to immediately issue a check to the political candidate for the same amount. If you analyze that particular employee's account, you'll generally find that the cash deposit is unusual and that the people involved hardly fit the profile of those who would be politically active — barely being able to pay their own bills, let alone make a campaign contribution. If you ask them to name the office of the candidate they donated to, don't be surprised if they don't even recognize the name of the candidate. That's because many may have been duped or coerced into participating, many not comprehending the severity of their actions.

Garden state of Eden

Even though it may seem like a symbol of corruption, New Jersey is hardly alone when it comes to trouble in paradise. From the Bible Belt to the Pacific northwest, with a detour through Louisiana along the way, political corruption knows no boundaries. AML professionals in every state of the union must remain just as vigilant as those of us in every corner of the garden state.

By the way, in November of 2009, Jon Corzine lost his bid for reelection. 

Charles Falciglia, CAMS, vice president/BSA officer, Mariner's Bank, Edgewater, NJ, USA, cfalciglia@marinersbk.com

The East African Community (EAC)

– Community effort is required to manage the risk of crime

A number of efforts have been undertaken in 2009 and are planned to continue in 2010 to bring East Africa economically closer together. In November 2009 the members of the East African Community¹ took a step in signing the law for the establishment of the East African Community Common Market. The law will become active in July 2010 and results in the free movement of labor, goods and services across the EAC's five member countries: Kenya, Uganda, Tanzania, Rwanda and Burundi. The economic union, which is being fostered in Eastern Africa, is a very positive development and presents great opportunities for the EAC's members and their long-term growth and development.

EAC peace and security

According to the EAC web site, the community has underscored the importance of peace and security in order to ensure a successful process of regional integration in regarding the control of cross-border crime. For this purpose, a Council on Interstate Security has been established in order to enhance cooperation. Key areas of focus include:

- Implementation of the Protocol on Illicit Drug Trafficking
- Small Arms and Light Weapons (SALW) Management Programs
- Cooperation in Police Matters

In December 2009, the United Nations Security Council called on the international community to strengthen cooperation with the UN and regional organizations in fighting the threat to

global security by drug trafficking, particularly in Africa. The statement also mentioned the growing concern attached to the link between drug trafficking and the financing of terrorism. The council also stressed the need to allocate resources in order to assist the East African countries in combating the threats faced by crime.

UNODC Report

In November the UN Office on Drugs & Crime (UNODC) published a report on *Organized Crime and Trafficking in Eastern Africa*². The background to the research was based on whether there are growing crime trends which are of concern and whether they pose a significant threat to the stability and societies of Eastern Africa³. The report aims to highlight trends and identify issues, which require a regional response, but leave room for individual national approaches.

The report summarizes its results as follows: *“Eastern Africa has experienced considerable progress toward sustainable development over the last years, but at the same time, the economic crisis, ongoing extreme poverty and inequality, climate change and a continuous threat of escalating violence and conflict in the region have continued to threaten Eastern Africa’s progress, and provide a fertile ground for the twin threats of organized crime and trafficking to flourish. Governments in the region have made efforts to develop and implement policies to turn the tide, but it is often the case that corruption, weak governance and rule of law have undermined those efforts.”*

Regional and political risk scenarios

Although the UNODC report highlights the considerable progress toward sustainable economic and human development in Eastern Africa, it underlines that Eastern Africa (see footnote 3) remains a conflict-prone region with the threat of new violent conflicts remaining high.

After many years of political tumult the EAC region is experiencing relative stability; however, political instability remains a risk. Eastern Africa borders three conflict zones: southern Sudan, Eastern Congo and Somalia, which given the wide spread trafficking of firearms, high influx of refugees and the general spill-over effects, increase the vulnerability of the EAC. Furthermore, conflicts taking place in the border region of Ethiopia are, according to the UNODC report, not diminishing significantly and therefore posing a long-term threat to the stability of the region.

The UNODC report claims that a persistent threat remains which could see Eastern Africa spiral into a vicious cycle of underdevelopment which is exacerbated by weak governance, weak rule of law structures and high level of inequality. It also notes that there is a significant amount of anecdotal evidence to suggest that the region is becoming an important transit location for illicit drugs and trafficked persons heading to the Middle East, Europe and elsewhere.

The risks highlighted by the UNODC are also reflected in a follow-up report published by the Security Council in November 2009.⁴ The report states that, according to the Secretary-General's Special Envoy for

¹The East African Community (“EAC”) is a regional intergovernmental organisation of the Republics of Kenya, Uganda, the United Republic of Tanzania, Republic of Rwanda and Republic of Burundi, and is headquartered in Arusha, Tanzania. The EAC was initially founded by Kenya, Tanzania and Uganda in 1967. It collapsed in 1977 and was not revived again until 1999. In 2007 Burundi and Rwanda joined the East African Community.

²http://www.unodc.org/.../easternafrica/.../Organised_Crime_and_Trafficking_in_Eastern_Africa_Discussion_Paper.pdf

³The report subsumes 13 countries in East Africa; Kenya, Tanzania, Uganda, Burundi, Rwanda, Djibouti, Eritrea, Ethiopia, Somalia, Seychelles, Comoros, Mauritius & Madagascar.

⁴http://www.securitycouncilreport.org/site/c.glKWLeMTIsG/b.5604085/k.DF30/Update_Report_No_1brNorthern_Uganda_and_LRAAffected_Areasbr13_November_2009.htm

community

the Lords Resistance Army-affected areas, Joaquim Chissano, the LRA attacks on civilians have increased in eastern Congo, Central African Republic and southern Sudan. These have led to an increased number of 'internally displaced persons' and refugees.

The report of the Secretary-General on children and armed conflict in Uganda published on 15 September stated that the LRA remains active in the region, as violence against civilians including killing, maiming of children, abductions, recruitment and sexual violence continues in the DRC, CAR and in southern Sudan. The report questioned whether the Security Council should take a more decisive stance on the issue.

AML legislation

In the lead up to establishing the common market, 2009 also saw various initiatives to meet international regulatory standards to combat crime pushed forward. In the field of anti-money laundering, Kenya saw the introduction of AML legislation, and in Uganda, a bill was presented to parliament in November and should reportedly be passed by parliament in early 2010. Kenya, Tanzania and Uganda are also members of the FATF's Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)⁵, which offers technical assistance and training. Tanzania, Burundi and Rwanda passed AML legislation between 2006 and 2008.

Newly enacted legislation and legislation, which has yet to be effectively implemented to combat financial crime, continue to leave ample room for criminals to benefit from the common market.⁶

Therefore, until strong institutions and enforcement have been installed, crime remains a serious risk within the EAC and Eastern Africa as a whole. A number of projects are underway and supported by the international community to provide assistance in implementing legislation and in setting up relevant institutions⁷.

The UNODC report also addresses the problem of combating money laundering in Eastern Africa. High costs and limited resources make enforcement nearly impossible. It also notes that addressing money laundering is complicated, as it requires excellent cooperation between a range of partners, national and international, and long-term resources that need to commit to lengthy, complex investigations. At the same time however, the report notes that it is not only the costs, but also the lack of political will and public pressure, as well as systemic corruption, which impedes the development and implementation of viable anti-money laundering regimes.

Money laundering is on the rise in Eastern Africa, despite international and regional initiatives and protocols. According to the UNODC report, money laundering methods include: securities trading, tax evasion, property purchase, cash and bogus sales transactions, as well as the embezzlement of public funds and a lack of prudence in the investment of public funds.


In Tanzania, for example, the equivalent of US \$16 billion was embezzled from the Bank of Tanzania's External Payment Arrears account in 2005.

In recent years, Kenya has seen several major corruption investigations, all of them relating to the former government, which allegedly stole millions of Kenyan

Shillings. Authorities in the UK have identified several people, who possessed fake diplomatic passports from the Ugandan Department of Finance, laundering funds in the UK.

Despite the concerns voiced by these more sophisticated financial crimes, it is worth mentioning, that according to the US 2009 *International Narcotics Report*⁸, the formal cooperation between counter-narcotics police in Kenya, Uganda, Rwanda and Tanzania is well established. Furthermore, the cooperation resulted in significant increases in effectiveness in each nation's narcotics control efforts. In 2008, Tanzania's judiciary reportedly convicted 467 individuals for narcotic offenses involving 'hard drugs' like cocaine and heroin, and 6,033 individuals for minor offenses involving drugs like marijuana.

The UNDOC report underlined that if money laundering is allowed to continue unopposed, that large sectors of a country's economy could end up under the control of organized crime. As a result, those same criminal organizations that control a country's economy would be in a position to undermine that country's democratic systems.

The following table published in the 2009 *International Narcotics Report* outlines which international instruments and standards on money laundering have been introduced into national legislation within the EAC. 

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

⁵See web site for further details: <http://www.esaamlg.org/>

⁶It is also worth noting at this stage that none of the EAC members have established Financial Intelligence Units, which are members of the Egmont Group (<http://www.egmontgroup.org/>).

⁷UNODC Project (2008-2009): *Measures to Combat Money Laundering and Financing of Terrorism in Three Eastern Africa States*. See following link for further details: <http://www.unodc.org/easternafrika/en/ongoing-projects/measures-to-combat-money-laundering-and-financing-of-terrorism-in-three-eastern-africa-states.html>. Regional Programme for Eastern Africa(2009-12) : *Promoting the Rule of Law and Human Security*. See following link for further details: http://www.unodc.org/.../Eastern_Africa_Regional_Programme_Final_Draft.pdf

⁸<http://www.state.gov/p/inl/rls/nrcrpt/2009/vol1/116525.htm>

Money laundering is on the rise in Eastern Africa, despite international and regional initiatives and protocols

High costs and limited resources make enforcement nearly impossible

	Burundi	Kenya	Rwanda	Tanzania	Uganda
Criminalized drug money laundering	N	Y	N	Y	Y
Criminalized beyond drugs	N	N	N	Y	N
Record large transactions	N	Y	N	Y	N
Maintain records over time	Y	Y	N	Y	N
Report suspicious transactions (“NMP”)	N	P	P	M	M
Egmont financial intelligence Units	N	N	N	N	N
System for identifying assets	Y	N	N	Y	N
Arrangements for asset sharing	N	N	N	N	N
Corporates with international law enforcers	Y	Y	Y	Y	Y
International transportation of currency	Y	Y	N	Y	N
Mutual legal assistance	N	Y	N	Y	N
Non-bank financial institutions	N	N	N	Y	N
Disclosure protection “safe harbor”	N	N	N	Y	Y
Criminalized financing of terrorism	N	N	N	Y	Y
States party to 1988 UN convention	Y	Y	Y	Y	Y
Intl. Terrorism financing convention	N	Y	Y	Y	Y

Y= Yes, N=No, M=mandatory reporting, P=permissible reporting

Train like a champion

A key component of an effective anti-money laundering (AML) program within a financial institution is the continuous training and development of its employees. Training employees on policies, procedures and controls is one of the four pillars of a functional AML program. Seeking out trends and recent guidance is crucial to staying ahead of organized crime and emerging illegal activity.

How is this feat achieved when illegal activity is consistently on the rise, the economy is in a weakened state, and companies are becoming leaner and cutting non-essential budget items? Generally, in times like these, the first budget line item that comes into the cross-hairs of a senior executive is the compliance training budget because training is usually seen as non-essential when budget items are discussed. Conferences and specialized training programs are steadily becoming fond and distant memories. Looking internally is a practical way for organizations to cut cost and optimize resources. But training has value that cannot be weighed in dollars and cents. As managers think about developing their AML programs, there are some main points to consider.

Developing topics

Knowledge is Free. Employees can share what they know with other AML professionals within the institution. Providing a knowledge-based forum for employees encourages an open exchange of questions and ideas among AML professionals that enhances overall regulatory and best practice knowledge. It also promotes continued knowledge sharing outside of the training environment by providing networking opportunities.

Although the training program provides relevant topics for AML employees, AML education should not be limited solely to AML professionals. Expanding AML knowledge can be beneficial to the entire compliance organization. Subject matter should be pertinent to the growth and development of the audience to enhance their knowledge and investigations. Schedule sessions that are "deep dives" into how your financial institution defines, investigates and/or complies with

AML-specific areas such as new regulations, structuring and the Bank Secrecy Act (BSA) to promote a level of understanding that may not be supported by daily job duties or cookie-cutter seminars. Ensuring facilitators incorporate case studies and an adequate balance between lecture and discussion are key factors in keeping the audience engaged. To avoid privacy issues, real life case studies should be cleansed of any non-public customer information and mention of SAR filings should be undertaken with care.

Getting leadership support

The support of senior leadership is crucial, as they are in the position to provide the necessary resources and "get the word out" of the vital significance ongoing training plays in a solid AML program. Every program needs a champion. A champion's role is to "go to bat" for the program. The champion believes in the purpose of the program, is dedicated to seeing the project implemented, and is willing to take responsibility for the outcome. The champion should be someone in upper management, or someone who has the confidence and support of upper management. This person will take the objective of the program to senior leadership to get their support. Without a champion, getting the program off the ground may prove difficult.

With the champion in place, the next step is to designate a program leader and organize logistical support. The program leader spear-heads all aspects of the training program. The program leader will seek out applicable topics, willing facilitators and valuable content among the many tasks he or she must perform. Strong time management skills and the ability to prioritize appropriately are also necessary, as the program leader will be handling training duties, as well as the normal work load. The program leader may choose to delegate some training tasks to balance out the responsibilities and engage other employees in the development of the program.

Making it happen – Logistics

Depending on the size of the organization, responsibility for logistical support

may fall under the responsibility of a department other than AML. A mid-size to large institution may have an education support division that can assist in this area. If participants in the training program are located in multiple geographic locations then logistic support becomes critical to the success of the program. When planning training sessions, the time of day is an important consideration. If participants are in different time zones, arranging a 9:00 EST training for employees on the west coast is undesirable, just as scheduling sessions during lunch time is a definite way to keep a training room empty. Internal research by the training area of a large financial institution has confirmed that sessions at the beginning or end of the week, as well as the end of the month, are generally not well attended.



During the development phase of the program, other factors such as the training session's location, the dissemination of materials and the length of the sessions are equally important. The training should be long enough to give considerable time for an in-depth discussion, but short enough to keep the attention of the audience. Use resources wisely and think

outside of the box. Training participants need not

attend in person, though you may find discussions are easier to facilitate when attendees are in one of a few locations. Sessions can be via live-meeting, phone or video conference. Congregating for sessions can enhance employee awareness, intensify topic discussions and increase networking.

Getting credit

A significant task for the logistic support is to keep a record of participants for each session. Make sign-in sheets available at all locations and forward

Speaking up

Finding the right internal speakers for specific topics can prove challenging. Networking and reaching out to diverse areas within your organization may assist in the process. It may be difficult to find facilitators to speak on topics that appeal to a wide audience. One starting point is to contact senior leadership to seek out recommendations for facilitators. This can be accomplished by generating a "call for facilitators" email, which is written by the program lead requesting suggestions for speakers to deliver specific topics. Numerous benefits come with facilitating a training session. A training session can assist potential facilitators with reaching developmental goals such as enhancing public speaking, becoming known as a subject matter expert, and networking. Senior leadership should encourage employees to consider owning a session to enhance professional development.

The program lead should assist facilitators with training content. This could include an initial discussion to talk about suggested key points that may be included in the session. Also, the facilitator should review a draft of the training content prior to the session. This will confirm all desired areas are encompassed, as well as ensuring adherence to company privacy requirements.

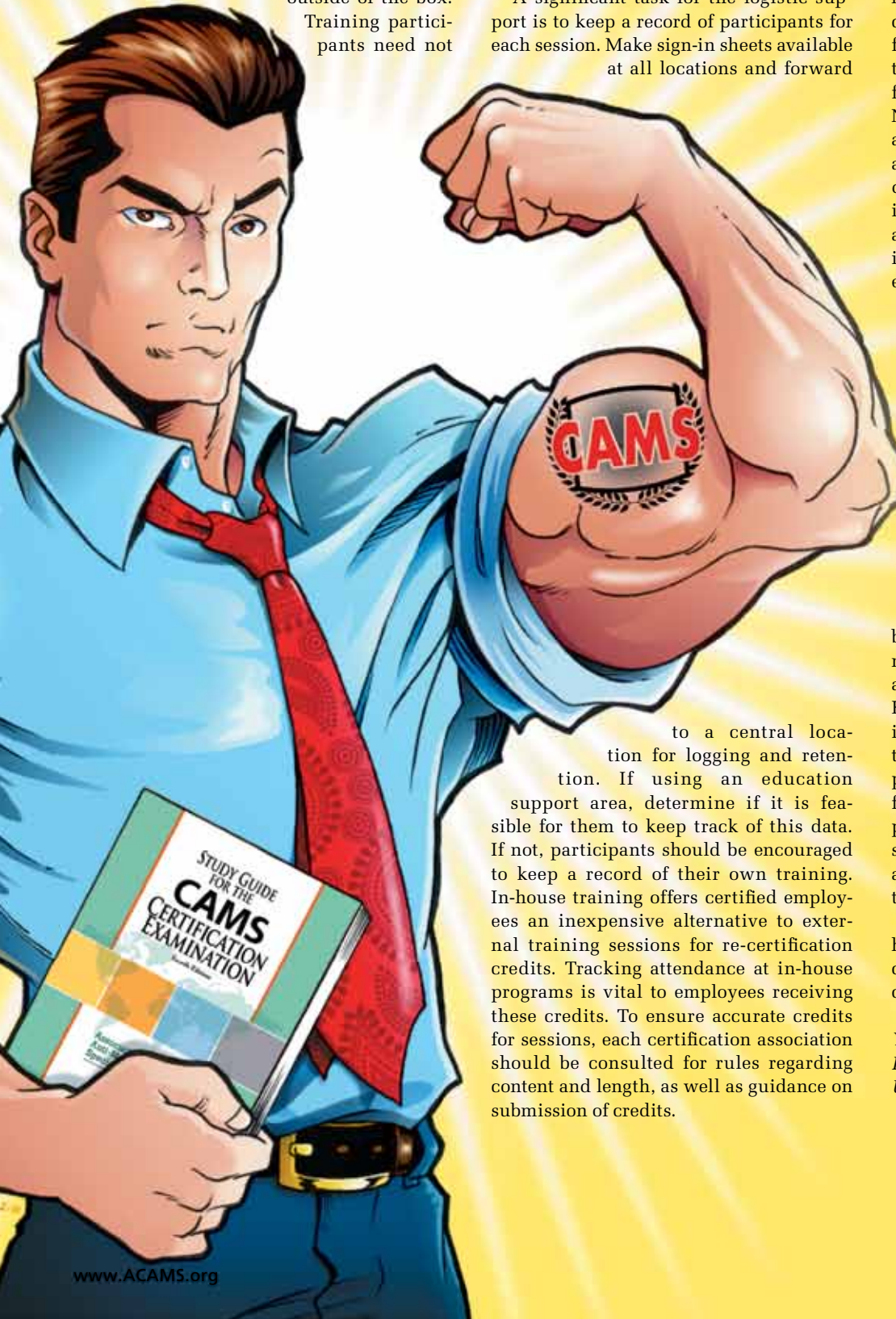
Improving and repeating

Once the program is instituted, feedback from participants is a prime way to measure the program's progress. Surveys are a practical way to request feedback. Key questions to gauge success should include; the length of the program, facilitator reviews, applicable course content and program improvements. Analyze the data from the surveys to adequately adjust the program as needed and ensure its ongoing success. Program improvements should be aligned with the overall goals and objectives of the training program.

The result will be a cost-efficient in-house AML training curriculum that is considered a critical component of the company's AML program. **A**

Yashica N. Whitehead, AML investigator II, Capital One Financial, Richmond, VA, USA, Yashica.Whitehead@capitalone.com

to a central location for logging and retention. If using an education support area, determine if it is feasible for them to keep track of this data. If not, participants should be encouraged to keep a record of their own training. In-house training offers certified employees an inexpensive alternative to external training sessions for re-certification credits. Tracking attendance at in-house programs is vital to employees receiving these credits. To ensure accurate credits for sessions, each certification association should be consulted for rules regarding content and length, as well as guidance on submission of credits.



Consolidated FIUs save institutions time, money and headaches

Despite fewer mortgage originations, mortgage loan fraud appears to be rising in the United States, with losses topping \$1.4 billion in 2008, according to the FBI.¹ In fact, mortgage fraud is the third most reported offense to the Financial Crimes Enforcement Network (FinCEN), with incidents spiking 44 percent in the 12 months ending June 2008. The numbers have remained steady since. What's more, a recent FinCEN study indicates a growing relationship between the individuals who perpetrate mortgage loan fraud and other financial crime activities.²

The number of reported fraud cases is expected to grow, as experts warn that losses will not peak until the latter half of 2010.

As mortgage fraud climbs, its economic impact is reaching financial institutions, lenders and borrowers. It is even beginning to trickle into communities. Mortgage fraud drains financial institutions' loan-loss reserves, profits, liquidity levels and capitalization ratios, while forcing lenders to increase mortgage pricing and fees to recoup loan losses. Furthermore, mortgage fraud artificially inflates home values and property taxes, creating long-term consequences for homeowners and communities.

To combat the problem, the federal government in fall 2009 established a nationwide mortgage fraud task force, combining the powers of four federal agencies and 12 state attorney generals. The Obama administration established the Financial Fraud Enforcement Task Force in November 2009. Led by the Department of Justice, federal agencies, regulatory authorities, and inspector generals will work with state and local partners to investigate and prosecute financial crimes, including mortgage fraud.

Lenders must take action in anticipation of the escalating loan fraud problem. They should look for ways to reduce costs and mortgage losses while creating long-term sustainable solutions agile enough to evolve even as fraudsters tailor their criminal activity to undermine new and improved controls. The solution lies in a centralized Financial



¹FBI 2008 Mortgage Fraud Report.

²Mortgage Loan Fraud Connections with Other Financial Crime: An Evaluation of Suspicious Activity Reports Filed By Money Services Businesses, Securities and Futures Firms, Insurance Companies and Casinos; Office of Law Enforcement Support, Financial Crimes Enforcement Network; March 2009.

Intelligence Unit (FIU) that consolidates the capabilities from mortgage fraud, anti-money laundering (AML), and other anti-fraud units while leaving necessary differences, such as transaction surveillance, decentralized.

A good first step to achieving this approach is to consolidate the investigation and case management of fraud across units. This provides insight into customer activity across lines of business with little disruption to current monitoring activities.

The fact that individuals committing mortgage fraud may also be linked to other financial crimes emphasizes the value of merging anti-fraud efforts to detect and prevent criminal activity.

An FIU that consolidates forces to fight all types of fraud, when established properly, could yield significant benefits. Shared services, tools, and personnel would reduce costs and risks. Improved controls and detection methods would stem fraud-related losses. Personnel would spend their time more effectively, and suspicious activity reports (SARs) would improve in consistency and quality. Ultimately, institutions would be better equipped to trace — and hopefully reduce — loan fraud.

Consolidated approach creates a distinctive solution

Mortgage fraud is dealing a damaging blow to the financial services industry, hurting community and large lenders alike. In the six months ending June 2009 the industry filed 32,926 depository institution SARs related to mortgage fraud, representing nearly 9 percent of all SARs reported during the timeframe.

Because mortgage fraud yields dirty money, it is no surprise that the same individuals reported for suspected mortgage fraud are often connected to other illicit activities, such as money laundering, check fraud, and structuring to avoid currency transaction reporting, according to the FinCEN study. Based on analysis of SARs filed between July 2003 and June 2008, of the 156,000 individuals reported for suspected mortgage fraud by depository institutions, interrelationships existed for SARs filed by non-depository institutions. These include an 85 percent overlap of SARs filed by money services businesses, 28 percent overlap for securities brokers/dealers, and 47 percent overlap for casinos/card clubs.

³MBA National Delinquency Survey, May 2009.

⁴“The Next Hit: Quick Defaults, More FHA-Backed Mortgages Go Bad Without A Single Payment,” Dina ElBoghady and Dan Keating, *Washington Post*, March 8, 2009.

Evolution of a fraudster

As the loan processing and underwriting rules and standards have changed during recent years, so too have the tactics fraudsters use to commit their crimes.

The frauds can be difficult to detect using traditional underwriting standards and involve highly organized rings of individuals. Fraud schemes can involve multiple complicit individuals, including borrowers, real estate professionals, property management companies, appraisers, loan officers, mortgage brokers or loan processors, title examiners and closing attorneys. And their schemes can include misrepresentation; illegal acquisition; or omission of information regarding credit, identity, income, assets, liabilities, property value, or occupancy status. Other methods include chunking, straw buyers, foreclosure rescue, equity theft, property flipping, affinity fraud, and “shot-gunning” frauds, to name a few.

At the height of the subprime mortgage boom, criminals took advantage of the opportunities to obtain loans in an environment that required low down payments and little documentation. The landscape was plagued with high-risk borrower profiles and less-than-trustworthy origination participants.

Today, the housing market opens the door to fraud through the FHA loan program, as reported by several sources. Nearly one-third of all new loan originations are FHA-insured loans, up from two percent in 2006. More than one in eight FHA loans are in delinquent status, nearly triple the delinquency rate of conventional, non-subprime loans, according to data from the Mortgage Bankers Association.³ And early payment defaults, loans where borrowers failed to make more than one payment, have nearly tripled in the past year on FHA loans, according to a *Washington Post* analysis.⁴ The industry regards early payment defaults as an indicator of improbity and fraud.

Barriers to a better system

Today, effectively fighting against fraud requires an enterprise-wide effort. Borrowing internal control best practices developed in the fight against other forms of financial crime can improve the prevention and detection of mortgage fraud. Although many lenders have implemented measures to catch fraudsters, at many institutions, methods have not adapted

to the evolving business, regulatory, and criminal environment.

Barriers include ineffective data collection and sharing, time, and the lack of aggressive adoption of sophisticated automated fraud detection systems.

Symptoms of these barriers include:

- Non-cohesive flow of information and knowledge captured throughout the loan approval life cycle
- Understaffing of mortgage fraud investigative units
- Suboptimal internal risk and regulatory reporting
- Inability to quantify and fully understand fraud related to actual losses incurred

The solution: The new Financial Investigative Unit

To adequately and efficiently curb mortgage fraud losses — as well as losses from other financial crimes — institutions should create a centralized and shared FIU that consolidates capabilities and maximizes the application of expertise across mortgage fraud and AML detection and control areas.

Institutions should consider centralizing the FIU to gain economies of scale across lines of business — focusing on providing account and loan origination customer due diligence, screening services, case management, and compliance information for regulatory reporting. At a minimum, each institution should integrate these types of processes into existing prefunding and quality control efforts.

The first order of business for the FIU, however, should be to focus on areas other than transaction anomaly detection related to AML and anti-fraud activities. These functions are typically the most dissimilar between units and may remain decentralized for each line of business. The FIU also should not solely focus on technology and/or process components. A number of other and equally important operating components, as represented in Table 1, should be on its agenda.

The centralized FIU will bring multiple benefits, including leveraging expertise and gaining economies of scale across lines of business. The FIU’s areas of focus should include providing account and loan origination customer due diligence, screening services, case management, the implementation and maintenance of more sophisticated mortgage fraud detection

PRACTICAL SOLUTIONS

Table 1: FIU operating components

OPERATING COMPONENT	KEY CONSIDERATIONS
Objectives and oversight structure	<ul style="list-style-type: none"> • Strategy, mandate and principles • Location (e.g., departmental and geography) • Governance and organizational structure
Management of Financial Intelligence Unit	<ul style="list-style-type: none"> • Escalation and dispute processes • Continuous improvement • Reporting – business unit, legal, and compliance stakeholder liaison • Risk management and mitigation
Operational and investigative technology/processes	<ul style="list-style-type: none"> • Case research, investigation, and disposition Fraud control and prevention framework • Fraud schemes and event triggers • Account opening/maintenance procedures • List management – internal (do not do business with) and external (ChexSystems) watch lists • Tool selection and points of integration • Screening (batch, ad hoc, account opening) and detection rules/analytics • Feedback loop of information to transaction surveillance, internal watch lists, and customer/account opening • Back-end reporting and monitoring processes • Post-/pre-production loan file quality control (QC)
Service level management	<ul style="list-style-type: none"> • Designing and negotiating key performance indicators, key risk indicators, and service level agreements (both internal with QC) and external with vendors • Service levels and incentives
Data standards and requirements	<ul style="list-style-type: none"> • Standards-based data collection model from surveillance and account opening systems • Standardized fraud taxonomy, risk model, etc. • Consolidating, homogenizing and indexing of customer, account and employee information from each line of business
Financial Intelligence Unit maintenance	<ul style="list-style-type: none"> • Review of unit performance • Business continuity plans, disaster recovery plans, record-retention requirements • Operational targets (productivity goals, quality levels, control metrics)
Financial	<ul style="list-style-type: none"> • Funding arrangements – financial operational plan
Human capital	<ul style="list-style-type: none"> • Roles and responsibility • Staffing, communication, training, and development of personnel • Regular monitoring of governance structure and compliance • Vendor management and outsourcing
Regulatory	<ul style="list-style-type: none"> • Privacy issues • Regulatory requirements (e.g., SAR reporting) • Notices and disclosures

engines, and producing consolidated fraud and compliance risk reporting for senior management and boards of directors. Many AML-focused FIUs have gotten quite expert and efficient in such processes and can contribute formality, process, IT know-how and case management rigor to anti-mortgage-fraud efforts.

With common tools, institutions can better deploy and cross-train existing staff. In time, AML and mortgage fraud detection staff can be consolidated into a single team able to adapt to peaks and valleys in work requirements.

Establishing an FIU creates a distinctive solution. By setting a single standard across all service lines, the reporting and resolution of cases becomes more consistent. Information that existed in siloed business lines becomes linked to allow more visibility into customer activities and potential fraud.

To achieve this transformation, institutions must take a number of steps in the areas of governance, information, screening, technology, and the supporting organization.

Key steps include:

Governance: Develop a fraud prevention framework and phased implementation plan across fraud types, products, channels, legal entities and geographies.

Information: Consolidate, homogenize and index customer, account, employee and related party information from each line of business. Improve quality and quantity of available electronic information.

Screening: Centralize watch lists and "do not do business with" lists across lines of business. Use link analysis to enhance screening and watch list filtering to include all parties to a loan.

Technology: Centralize screening, case management, investigative, and reporting capabilities while maintaining line of business legacy detective technologies.

Supporting Organization: Transfer screening and watch list filtering responsibility at time of origination from account officers/loan officers to a due diligence officer.

Key challenges

The current nature of anti-fraud units poses some challenges in implementing an FIU. Many institutions lack a consistent definition of fraud. It means different things to different people and covers a wide variety of schemes, actors, proxies,

channels, products, services, regulations and lines of business. Traditionally, compliance departments have responsibility for AML, while risk management groups oversee other fraud units. Because of the links between the two, ownership must be coordinated.

Different regulations and rules across different fraud areas means that the FIU should set a standard process that is acceptable for compliance, risk managers, and the lines of business. By starting with the most conservative approach for all fraud control units, a minimum regulatory requirement can be met.

Conclusion: FIU yields high reward with low pain

The escalating losses attributed to mortgage fraud cannot be ignored. Neither can the perpetrator's link to other financial crimes. Financial institutions must seek solutions that will address the challenges head on and can be adjusted to changing issues and events that develop over time.

Just as breaking down silos in other areas of the business leads to increased consistency, cost savings and reduced risks, so too can an FIU create these benefits for cases of fraud.

When implemented appropriately, an FIU provides substantial benefits in the following areas:

Costs savings

All banks have personnel and infrastructure to perform the tasks related to fraud controls across separate areas of the organization. Several of these tasks overlap, and an FIU can consolidate these functions in a single place. The degree of savings depends on the number of redundant personnel, systems and processes. If an institution consolidates only a few of the redundancies, the full benefits of cost savings may not be realized.

Reduced risk

An FIU with consolidated case investigation, review, and disposition, provides visibility into customer activities across the lines of business. Case managers can then identify suspicious activities through linked accounts or similarities between cases that might otherwise seem benign. Also, anti-fraud activities that were the responsibility of the account officer or loan officer would be moved to a shared

FIU. Due diligence and screening could be improved with this shift, eliminating potential conflicts of interest.

Reduced losses

By improving the loan origination process, it is less likely that fraudsters will be able to complete a loan transaction, thus curbing losses up front (losses associated with owned assets, as well as repurchase or make-whole-related losses from investors). However, if a fraudster is able to acquire loan approval, the ability to detect and resolve the fraudulent activity is accelerated, reducing the likelihood of repeated activity that could result in more significant losses.


Increased efficiency

If an FIU bears the responsibility for fraud detection, loan officers can reduce the time they spend on anti-fraud activities and turn their attention to more profitable tasks. Also, as case managers gain more insight into customer activity within and across business lines, they can reduce the time it takes to clear false positives.

Improved SAR quality and consistency

Because one unit files SARs for both AML and mortgage fraud, the reports become more consistent. Also, a single set of procedures enables more consistent research, investigation, review and disposition of cases. In turn, the quality of SARs increases because the wider lens into customers across different units allows visibility into potential patterns of interest.

Improved customer understanding

By linking customer accounts across units, organizations will have the insight and ability to quantify how customers who conduct business across units affect the organization when fraud occurs. Organizations will no longer view customers in silos, without the ability to trace activities in different areas. 

Jeff Lavine, Partner, Pricewaterhouse Coopers LLP, Tysons Corner, VA USA, jeff.lavine@us.pwc.com

Thomas Messina, Director, Pricewaterhouse Coopers LLP, New York, NY USA, thomas.messina@us.pwc.com

Peter Pollini, Principal, Pricewaterhouse Coopers LLP, Boston, MA USA, peter.c.pollini@us.pwc.com

Developing the investigative mind

A villain thinks like a villain. He does bad guy things. They spend their day thinking up more villain things to do. They associate with other villains and do more bad things. One of the advantages of being a villain is when a villain gets an idea, they can try it out immediately and if it does not work, they can analyze, alter and correct it and try it again tomorrow or try something completely different any time they want. They play by no rules or regulations; nor do they follow any policies or procedures.



The good guys, conversely, have an anvil around their necks. Firstly, there is always the issue of funding. I'm sure I don't have to remind anyone reading this that prevention is always last in the budgetary chow line. Further, there is the inherent issue that good people tend to think and act like good people. Most of us are not familiar with the villain realm (an advantage for the villain team). The usual game plan for the good team is to fix all known problematic situations. Many times I have heard one of the good guys say something to the effect of, "we have policies that deal with that." Or, "we have top of the line software", or "that has never happened before." However, while you may have policies against the usual suspects, transgressions, incursions, or any known issue, problems manifest because it is the unknown or the future issue that arises. The issue that you are not yet aware of is the most dangerous. Your reference for criteria is only effective on known problems and based on good guy thinking. Just because the good guy cannot think of a problem issue, does not mean that the villain has not or will not.

Herein lies the crux of a very common problem in compliance. There is a lack of strategic thinking. We usually don't have a unit assigned to play the role of the bad guy (if they even could) other than some basic quality control (which only assesses known problematic situations). I am talking about real strategic thinking that allows a unit to be free thinkers and

provides them with the means to truly go outside of the box.

Let me provide an example. As all of us in the AML world know, or should know, a quality anti-money laundering (AML) program usually begins with the Customer Identification Program (CIP). That's great, except all subsequent hard AML work goes out the window if the bad guy used fictitious identification. Perhaps you believe that you have solved all your worries by implementing a biometric iris scanner. Good guy: "Hey we finally beat the villains, now you can

only assess your account by putting your eye up to a scanner." Villains: Those fools don't realize that computers operate on a binary system. Everything is transformed into a pattern of digits. If we hack into their system and compromise them at the source, we will have everyone's iris identifying information and we can steal their identities forever...cool."

Like I said, it's always a matter of preparing for the unknown. I remember going through the State Police Academy many moons ago and some old crusty Sergeant said to me, "Son, you don't know what you don't know." Boy, was he ever right!

Now you may say, let's hire some villains to get their input. I am not a fan of this concept. I would rather hire the investigator that arrested the villain, or the attorney that prosecuted them. Admittedly there may be some advantages to consulting with a villain; however, I would hesitate to give him the keys to the kingdom. While some may say that the former villain has paid their dues and has seen the light; that might be so. I will remind you that he usually is only remorseful because he got caught. Not too many villains, particularly, white collar criminals, have walked into the front door of the police station and said, "Here I am and I'm sorry for what I have done, I surrender, and I'd like to make it up to society by working for the good guys now."

Furthermore, that mindset, the let's give the bad guy a chance, flies in the face

An AML director from a progressive bank does something very progressive. He has his staff spend some time each day exploring the Internet. Going to new sites, clicking on various advanced setting buttons and generally becoming more aware of the Internet and its sources of information. The rewards surface when enhanced due diligence is required and the staff can navigate to where they need to go quicker and with more accuracy.

of the number one rule below — be suspicious. This is exactly the mindset that I am talking about. Being forgiving works well in church, being suspicious works better in risk assessment.

(I should say that I can be fickle and I did change my mind about one former villain. I had the opportunity on a couple of occasions to meet and chat with Frank Abagnale of “Catch Me If You Can” fame. I realized that he did what he did as a 17 year old kid and he did it for himself and not as part of an organized criminal element. After Frank paid his dues in prison, he spent the next 35 years assisting law enforcement, for free, long after his sentence was completed. Subsequently, his son has gone on to serve in law enforcement. No excuses here, he was wrong for what he did, however, as tough as I can be with my suspicions and assessments, my instincts tell me that he is a very bright man who did something dopey as a kid and ultimately found his way to the straight and narrow. I’m sure there may be other reformed bad guys out there, just be careful if you should choose to avail yourself to this.)

So what then is an AML professional to do? A key phrase is “using your instincts.” Good instincts are part of developing the investigative mind. Your instincts come from your environment, experience, knowledge and ability. We are not born with investigative instincts, they are developed. As I mentioned earlier, good people think like good people. This is why I sometimes bang my head against the desk when I read some of the AML blogs or listservs where it appears that certain people and/or entities that are being investigated are given the benefit of the doubt or excuses are even being created for them by the people who are assigned the task of investigating them.

Stop right there! It is not your job, nor mine, to determine guilt or innocence. It is our job to obtain the facts and report the same. When we don’t have all the facts (and you usually don’t) you make use of all your “instincts.” While instincts have no place in the court of law, they sure should take front and center while you are completing an investigation. The more experience and knowledge you have, usually, the greater your instincts. Follow your instincts, go through doors, open windows, turn over stones but find as many of the facts as you can without predisposition and/or prejudice. If something does not feel right, then try to figure out why. Be suspicious yet judge slowly.

Here are some thoughts on developing your investigative mind:

“The temptation to form premature theories upon insufficient data is the bane of our profession.”

— Sherlock Holmes

1) Be suspicious, be suspicious, be suspicious. The case has come across your desk for a reason. Somebody or some software has viewed this case as unusual, or odd. It is up to the investigator to review, analyze, research, investigate, then report.

We all understand a person is innocent until proven guilty. However, this is not the court of law. I’m suspicious of everyone, at least until I can confidently cross them off my list. I cross them off by completing a thorough investigation, not by guessing, assuming or being captivated by a nice smile. Remember, bad guys try to look and act like good guys. I’m sure there are some who might feel that this is a terrible way to live. I’m not suggesting that you live your life suspicious of everyone all the time, you can turn it off when you leave the office. Being like Aunt Bea from *Mayberry* is just not good enough if you want to be an effective investigator. The Investigator’s job is to discover the facts as best as he or she can. Each case should be approached with suspicion on the mind, but with neutrality and evenhandedness as your course of action.

2) The smell test. If you think it stinks, it probably does. You do this job every day, you work with people who do this job every day, if for some reason, the hair on the back of your neck is standing up, then go with the feeling. You are probably right. Understand, of course, that hair standing up on the back of your neck is not a valid probable cause in the court of law, so you do need to be able to articulate your feelings. What is making you feel this way? Figure that out, then run with it. This goes back to instincts. Don’t be too quick to dismiss your gut feelings. If you can’t figure it out, ask a new set of eyes to take a look. Don’t be embarrassed to ask. I have yet to meet anyone who resembled Sherlock Holmes and has all the answers. We can all use a little assistance from time to time.


3) The Investigator must understand that by only considering one hypothesis then he or she may be missing the boat. You must begin the case entertaining numerous possible hypotheses. The more

knowledge you have about current trends and patterns then the more hypotheses become available. Keeping up with and abreast of the latest and greatest techniques and methods is very important.

4) Make available new sources of information and/or technology. This might be more difficult as it usually involves spending budget money. However, there are other things that you can avail yourself of such as local meetings with your peers and law enforcement, various free seminars and webinars and trade magazines and publications.

5) “There have never been any cases before like this,” or “No one has been arrested for this type of activity previously.” Did you ever notice whenever some nutcase goes on a shooting spree, the TV news interviews the neighbors and they always say the same thing...he was such a nice guy, we never knew of any problems... yada, yada. You are not being paid to be the clueless neighbor; you are being paid to keep the place secure. Your job should be to envision the possibilities and create a path of action to prevent disaster. Refer back to rule number 1.

6) J.A.D.E. – Justify, Articulate and Define Everything. Assuming that you no longer have the “Pollyanna, everything is wonderful attitude,” and have morphed into the “I’m suspicious of everything that moves attitude.” then you need to follow the JADE rule. In an investigation everything you do is memorialized. You never know where that file will end up; executive board, law enforcement or courtroom. You have to justify all your actions and further articulate and explain why you did what you did or why you did not do what you did not do. Your results will be defined and ultimately an action will be taken (note that even inaction needs to be defined).

Good people always wonder, how can the villain think like they do? Conversely, the villain wonders, how the heck can everyone else be so gullible and soft? That’s just the way it is. Fortunately, we have some very fine people on the front lines both in law enforcement and in the risk, compliance, and AML side of the financial sector. I wish you the best of luck in the constant battle between good and evil. Keep your sense of humor, stay alert and be diligent. 

Kevin Sullivan, retired Investigator from the NY State Police, Director of the AML Training Academy, New York, NY, USA, Kevin@AMLtrainer.com

Collective Entity Resolution:

Raising the technology bar
for watch list filtering



The importance of vetting and aggregating data from multiple sources to understand exactly who you are dealing with, was instantly highlighted this past December with the attempted terrorist attack on Northwest Flight 253. A presidential report to the American people revealed that although the suspect was known to U.S. counter-terrorism authorities, his name was not properly checked against government databases. What's more, a misspelling of his name prevented him from being identified as holding a valid

U.S. visa that allowed him to travel to the United States. Intelligence reviews further attributed the problem of identification to "fragments of data", "disparate pieces of data [not] being assembled," "the watch list process [not being] fully connected to counterterrorism analysis" and "[no] constant reviewing of watch list data."

The inability to "connect the dots" from disparate data sources and non-obvious relationships in data across multiple silos is precisely the problem that collective entity resolution solves.

Entity resolution defined

Entity resolution, also known as "identity resolution" or "record linkage," analyzes all of the information relating to entities (e.g., individuals or companies) from multiple sources of data. It then applies likelihood and probability scoring to determine which identities are a match and what, if any, relationships exist between those identities. More simply put, entity resolution is the process of aggregating and grouping records that represent partial representations of the same entity.

Figure 1

The Traditional Approach Matching Records Independently

SOURCE	UID	FIRSTNAME	LASTNAME	ADDRESS1	ADDRESS2	CITY	STATE	COUNTRY	SCORE	DECISION
CIF	1234567	ALPHA M	SOUMAH	c/o BOKE SERVICES	30 ISBELLA ST	PITTSBURGH	PA	USA	92	?
PEP	9876543	ALPHA MADY	SOUMAH					GUINEA	92	?
CIF	5432109	IBRAHIMA	SOUMAH	c/o BOKE SERVICES	20 STANWIX ST	PITTSBURGH	PA	USA	95	?
PEP	5678901	IBRAHIMA	SOUMAH					GUINEA	95	?

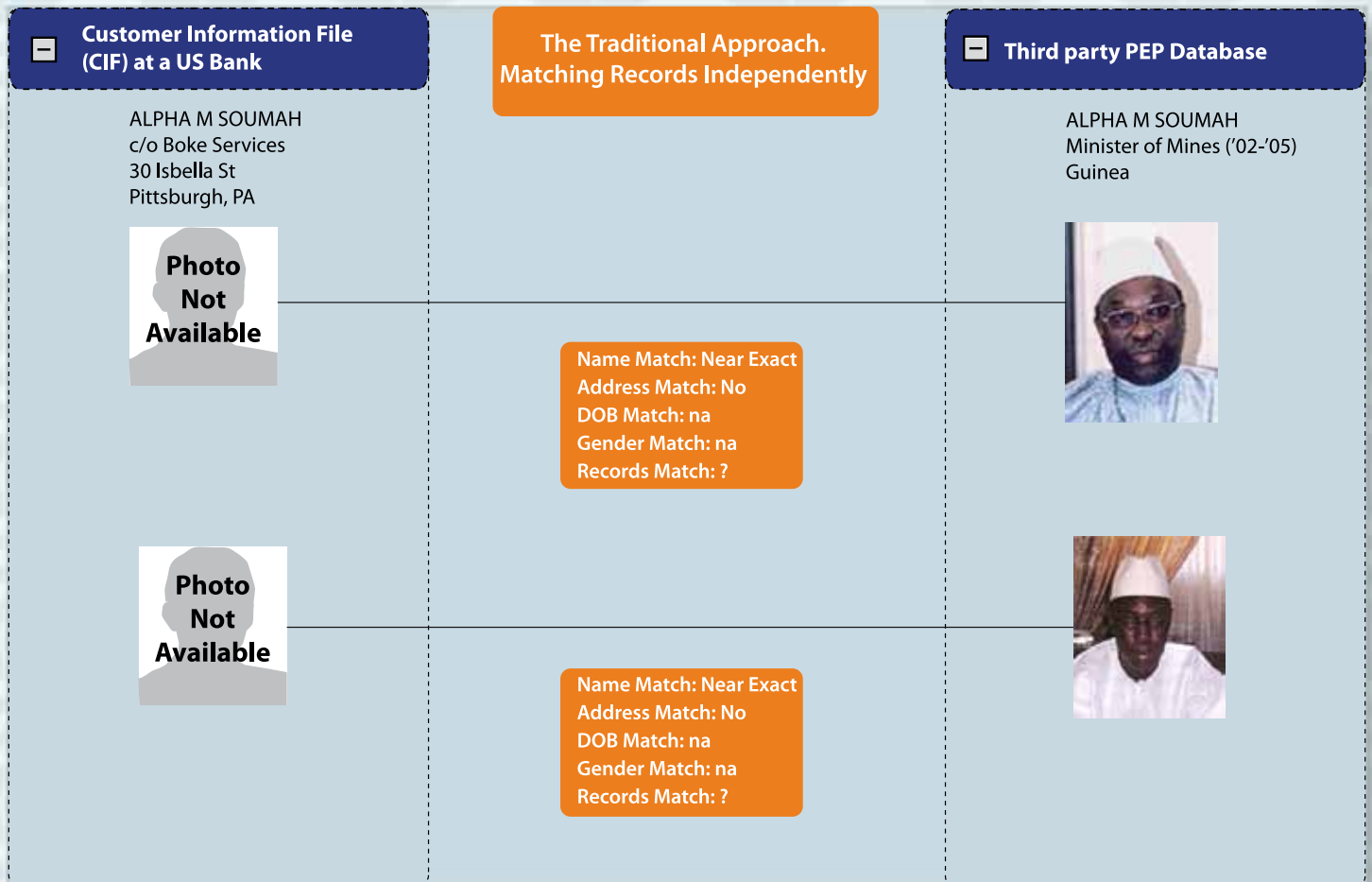
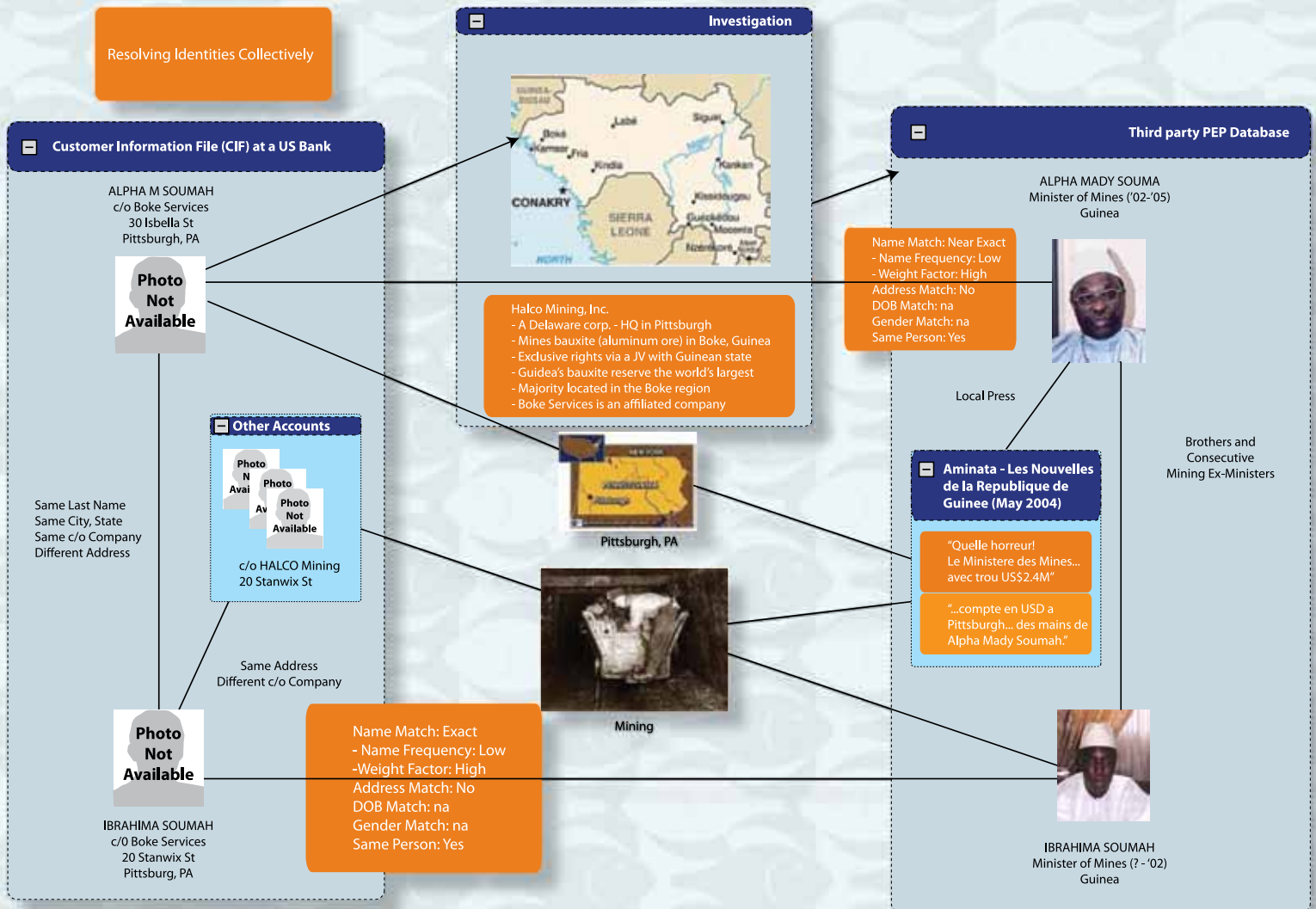


Figure 2



The goal of entity resolution is to reconcile database references that correspond to the same entities. The process is challenging because relationships are not always obvious and the data is prone to error and variation. The challenge is exacerbated when no unique entity identifiers are available, as is generally the case with watch-list screening. Entity resolution becomes collective when resolution decisions are dependent on one another through relational links. Relational links are connections between entities.

Challenging the traditional approach

Watch-list filtering technology, with its many algorithms for name matching, is frequently used to screen customer files against government sanctions lists and large databases of high-risk entities. The information contained in these large databases must be summarized and synthesized in order to support decision-making. Name matching solutions commonly use pair-wise comparisons. This approach resolves entities using pair-wise comparisons of reference attributes, such as

name, address or date of birth values. The absence of sufficient attributes will generally cause false positives.

In the first example of the Soumah brothers case study [Fig. 1], records are matched independently. However, there is often additional relational information in the data with references to different entities. The second Soumah brothers illustration [Fig. 2] shows how entities with coincidental references are determined jointly rather than independently. Known as clustering, this entity resolution methodology differs



from pair-wise comparisons by using both attribute and relational information to improve the accuracy of entity resolution. This real-world case study presents a strong argument for collective entity resolution as the next generation of watch list filtering.

The new frontier

In its predictions for the year ahead, BankInfoSecurity.com lists Bank Secrecy Act/Anti Money Laundering (BSA/AML) enforcement as one of the top five regulatory trends for 2010. While regulators focused on the capitalization and liquidity of financial institutions in 2009, it is expected that attention will return once again to the core compliance issues of BSA/AML. Government mandates direct financial and other institutions to avoid doing business with known “bad guys.” For these institutions, the Know Your Customer (KYC) and Enhanced Due Diligence (EDD) challenges include dealing with large dynamic databases with frequent updates, incomplete and incorrect records and known name variations across multiple data sources, among other issues. When choosing a watch-list filtering solution, if the goal is to do the minimum in order to be in compliance with the regulations, then most data matching offerings will meet these requirements, although one may spend significant time and effort reviewing false positive alerts. If, however, the goal is to find “bad guys” by “connecting the dots” to identify non-obvious relationships, and to make use of all available record attributes and relational information to reduce false positives and prioritize high risk alerts, then advanced technology using entity resolution techniques is worth looking into.

Solutions that provide sophisticated relationship detection and resolution can be distinguished from basic pair-wise data matching software by the following features:

- Works with both structured and unstructured records
- Uses comprehensive business rules to deal with missing, conflicting and corrupted information
- Utilizes non-matching, linking information in addition to direct matching
- Uncovers non-obvious relationships and associated networks, i.e., who’s associated with whom

These features are especially effective for terrorist screening, fraud detection, USA PATRIOT Act compliance, organized crime and drug ring detection and customer/applicant screening. Entity resolution technology on the market today varies in features and functionality. In the same way as human analysts use names, addresses, dates, identity numbers and other data, the system must be able to use matching algorithms that effectively rank, score or eliminate the potential matches. A robust solution will address identity matching, relationship detection and resolution, manual alert remediation and business process integration.

Specialist technology providers in the AML and compliance arena recognize a growing trend in unique customer data-matching needs. Institutions are looking for smarter, more efficient ways to implement and automate these processes. In an era of electronic transactions, global markets and online banking with customers entering their own information, data quality will continue to be an issue. KYC and EDD could become

increasingly time-consuming and costly. Consider how the ability to “connect the dots” and identify those individuals, entities and relationship networks with the highest relevance and probability of being true will produce the results needed to stay ahead of the risk.

Gartner, a leading research and consultancy firm, has been tracking the entity resolution market for several years. Their July 2009 report, “Hype Cycle for Master Data Management,” states that although previously considered an obscure technology, world events and market forces have pushed entity resolution to the forefront. As such, collective entity resolution techniques may soon be considered best-in-class for watch list filtering. **A**

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



VIRTUAL WORLDS

-A tool for money laundering and terrorist financing?

In 2006, *BusinessWeek* magazine featured the avatar Anshe Chung on their cover. Why? In just over two and half years, Chung had taken her investment of US \$9.95 and successfully became the first person to earn a net worth exceeding US \$1 million from profits entirely earned inside a virtual world¹.

KZERO, which is a worldwide virtual global consultancy and analysis firm, estimated that as of February 2009, there were more than 400 million virtual world users worldwide, with more than 25 percent of users playing more than thirty hours each week.^{2,3}

To understand the virtual world arena, one must understand the various aspects of a virtual world community, the players and the different virtual world concepts. The term “virtual worlds” is broad and can refer

to massively multi-player online games (MMOs), massively multi-player online role-playing games (MMORPGs), as well as massively multi-player online real-life/rogue-like games (MMORLGs), which all allow users to operate in an Internet-based environment and interact with other users.⁴

MMOs are interactive games that allow for the participation of thousands of players.

MMORPGs allow the user to play a specific character, which is the central character within the game, whereas MMORLGs, allow for the user to edit and alter a character, which allows the user to play various roles throughout the course of the game. Avatar is another name for a user’s character representation within the game. It can also refer to the personality or the screen name of the user and can be akin to a digital version of a user’s personality.

There are several different types of virtual worlds ranging from blogs to social mediums to chat rooms to forums. Some of the more popular virtual worlds include Second Life, which is a social networking site that has over 12 million registered users, World of Warcraft, which is a fantasy platform and has approximately 10 million subscribers, Guild Wars, which is

¹“My Virtual Life” *BusinessWeek* 1 May 2006.

²<http://www.virtualworldsnews.com/2009/02/k-zero-260m-registered-accounts-for-the-1015yearold-virtual-world-demo.html>, accessed 2 January 2010.

³www.nyls.edu/“Escaping the Gilded Cage: User Created Content and Building the Metaverse” 2004-2005

⁴<http://www.ecommercetimes.com/rsstory/61893.html?wlc=1264192743>, accessed 2 January 2010.

Full Day Anti-Money Laundering Seminars in Spanish

This series of one-day Spanish-language seminars is for AML/CTF professionals in Latin America; including newcomers in the field who want to learn the fundamentals of AML to veterans looking to stay up-to-date on the latest developments and best practices.

The seminars explore the regional AML landscape, as well as the latest global developments that impact the region and recent cases and money laundering methods.

Register by
April 2
& Save

\$50

Mention VIP Code
1BAL01

Benefit from a full day of practical learning*

- Get updated on the latest AML developments and best practices in the region
- Learn how to keep your institution compliant with AML regulations
- Speak with top level professionals and learn from their personal experiences
- Learn the strategies and elements of a solid AML/CTF program
- Earn continuing education credits for your professional growth

* These seminars are conducted in Spanish

BONUS: FREE 2-week trial subscription to Lavadodinero.com with seminar registration.



San José

March 5



Montevideo

March 26



Panamá

April 23



Bogotá

May 21



Santiago

June 18

another fantasy site that has approximately 2 million players, Cyworld, which is a relationship type platform, and SmallWorlds which is a social networking site with approximately 2 million users.^{5,6}

In regards to “virtual currency,” there are several virtual worlds that operate with this mechanism to allow for trade within their particular virtual world. This works by allowing the user to purchase the virtual currency through a credit card or an online payment system such as PayPal. Second Life has implemented the “Linden Dollar” or “L\$”, Cyworld trades in “acorns”, World of Warcraft trades in “WoW Gold” and Guild Wars trades in “Guild Wars Gold.” Some virtual worlds have implemented exchange houses to facilitate the exchange of currency. Second Life has implemented a currency exchange called “LindeX” which allows users to exchange multiple real world currencies into virtual currency, as well as trade other virtual commodities. The exchange rate is approximately 300 “Linden Dollars” to 1 US dollar. Second Life also allows users to earn “Linden Dollars” by selling virtual items.

Vulnerabilities associated with virtual worlds

Numerous vulnerabilities plague virtual worlds that allow for criminal groups and terrorist organizations to insert funds through this mechanism: 1) the avatar allows a user to mask his or her identity and allows for anonymity, which in turn proves to be difficult for law enforcement to detect the user’s true identity; 2) the majority of virtual worlds users participate in Internet cafes or in public spaces, providing yet another way for users to mask their identities and make it difficult for law enforcement to locate a user; 3) virtual currency in some virtual worlds can be converted to real world currency, which has the potential to allow for individuals to use this mechanism to mask the origin of their funds; 4) there are no regulations within these virtual worlds that mirror regulations in the financial world to safeguard against financial crimes and terrorist financing; 5) these platforms allow for numerous individuals to work with each other to create financial schemes, possibly using avatars that give no connection to their true identities; 6) virtual worlds also allow for the rapid transfer of information and virtual currency across international

and national boundaries, which has the potential to transfer funds, information and virtual commodities between players that increases the anonymity of these transactions and makes it very difficult to trace the origin of the funds; 7) users can easily use stolen credit card numbers or prepaid cards loaded with illegally gotten funds to open their accounts within these virtual worlds.

The interest and concern for the use of the virtual world, to include the use of the Internet and other virtual mediums, by terrorists and other criminal syndicates is not new. In April 2007 INTERPOL, the international law enforcement organization based in Europe issued a warning that “as a matter of urgency” law enforcement needed to increase their vigilance in respect to the criminal use of virtual worlds.⁷

In February 2008, Andrew Cochran, Co-chairman of the Counterterrorism Foundation, moderated a panel before the Chairman of the House Homeland Security Committee entitled “Meta-Terror: Terrorism and the Virtual World,” which included experts in the field to discuss the potential worldwide security implications of the use of virtual worlds by terrorists and criminal groups. Virtual worlds were highlighted for their use by terrorists as a tool for recruitment, training, and as an avenue for financing, which was noted as the most useful tool, due to the ease of transferring funds from one user to another.⁸

Virtual gaming companies realize that compliance and regulations need to be enforced. In September 2008, Second Life created a regulation which prohibited banks and ATMs within Second Life to offer interest on investments without proof that the banks and ATMs were registered with a government, or had a financial institution charter.⁹ This regulation was due to the fact that in August 2007, Ginko Financial, which was a “virtual investment bank” that produced investment returns of up to 60 percent, disappeared and Second Life players who had invested with Ginko Financial lost approximately US \$75,000.¹⁰

Possible best practices and recommendations


What are the solutions to combat these vulnerabilities? One, Internet cafes and public spaces should require customers to present identification to document who is using the computer. Of course, individuals could use false identification to circumvent

this requirement. As mentioned before, some virtual worlds allow the user to convert virtual currency to real world currency, which opens up the potential for money laundering and terrorist financing. These platforms should be subject to bank licensing regulations to insure users that funds are safeguarded or allow for requirements in the amount of funds that can be taken out, similar to a financial institution.

A compliance department should be implemented to oversee virtual transactions within any virtual world medium, thus requiring suspicious transaction reports to be filed, implementation of proper know your customer procedures, as well as other financial regulations. Additionally, this compliance department could work closely with law enforcement in finding criminals or tracking down those users who are injecting illicit funds or attempting to launder money through these virtual worlds.

If conducting any type of financial transaction within the virtual world allows for a user to convert the funds to a real world currency, the user should be mandated to provide his or her identity to track these transactions and to prevent excessive withdrawals or suspicious activity. The most reliable way to stop the potential for money laundering and terrorist financing within these virtual worlds is to eliminate the ability of a user to exchange virtual currency into real world currency — though strict, it would stop the potential for terrorist financing or financial crimes to be conducted by a user.

Jurisdictional boundaries and laws addressing virtual worlds need to be established, so that countries can prosecute those users who exploit virtual worlds to launder funds or use funds to support terrorist groups and their activities.

We are well beyond the information age as a perfect tool for terrorist groups and criminal syndicates. The increased use of the Internet, virtual worlds and other electronic mediums will only increase. It is important that we anticipate the changes introduced by our technological world and stay a step ahead in regards to regulations, vigilance and reporting so that criminals and terrorist groups cannot take advantage of these mediums for their own benefit. 

Heather A. Brown, CAMS, Washington, D.C., USA, HABrown35@aol.com

⁵<http://www.crunchbase.com/company/smallworlds>, accessed 2 January 2010.

⁶<http://www.mmogchart.com/analysis-and-conclusions/>, accessed 2 January 2010.

⁷http://www.world-check.com/media/d/content_pressarticle_reference/Virtual_Worlds_Clear_and_Present_Danger_for_Money_Laundering.pdf, accessed 2 January 2010.

⁸http://counterterrorismblog.org/2008/03/event_transcript_and_related_1.php, accessed 2 January 2010.

⁹Florida Department of Law Enforcement, Office of Statewide Intelligence, Tallahassee, Florida

¹⁰http://www.wired.com/gaming/virtualworlds/news/2007/08/virtual_bank, accessed 26 January 2010.

Chapter Development Department

A *CAMS Today* spoke with Catalina Martinez from the chapter development department to discuss what is in store for ACAMS' Chapters in 2010.

Catalina Martinez is known by "Kata" to many of her colleagues and ACAMS' members. She is the chapter development manager and like many at ACAMS she wears many hats and is also the task force liaison.

Martinez has over eight years of experience in working with associations and she has assisted in the launching of several ACAMS chapters.

AT: How many ACAMS' chapters exist today?

CM: There are eight active chapters running now and of those eight, five have been launched since September 2008.



AT: Will there be more ACAMS' chapters formed in 2010?


CM: Yes, we plan to launch four more before the end of 2010. The first two: the Canadian Chapter and the Boston Chapter will be launched by mid-2010. We are also planning to expand into Europe, Latin America and the Caribbean.

AT: What are the benefits of joining a chapter?

CM: Chapters are meant to be another one of our many member benefits, but intensified to the ninth degree. We've fused together the learning and networking aspects of our larger live events onto a smaller scale for our members in different regions of the world. For a minimal yearly membership fee, which goes in its entirety to the support of the chapters, members

can attend most learning events for free. Also, Chapter members can earn CAMS credits, network and learn in just a couple of hours before, during or after work.

AT: Is it difficult to launch a chapter?

CM: It's a labor of love. You have to love what you do, love to help others and be willing to give of your time to do it. I do not know if members realize it, but our executive board members volunteer their time to help run these chapters with the help of ACAMS. We offer all the support a chapter executive board will need but in the end, they're the ones that make it happen. Believe me, when I say that none of this would be possible if it were not for our chapter executive board members. We are extremely happy with what they have accomplished thus far. Chapters are run by our members for our members. 

April 28-29, 2010 | Metropolitan Hotel | Toronto

The Canadian Institute's

9th Annual Forum on

ANTI-MONEY LAUNDERING

PRACTICAL STRATEGIES TO REDUCE RISK AND ENSURE COMPLIANCE



To register visit

www.canadianinstitute.com/AML3 or call 1-877-927-7636

Priority Service Code: DA406ACAMS

Hear from regulators, law enforcement, top financial institutions and leading lawyers on key topics including:

- The latest from FINTRAC, OSFI and IIROC on their current initiatives, priorities and expectations
- The nuts and bolts of risk-based assessment
- Case studies, typologies and the international perspective
- Q&A session with the regulators

Keynote Speaker:

Jeanne M. Flemming,
Director, FINTRAC

Members of ACAMS receive a 15% discount.

This event qualifies for up to 16 CAMS Credits

Carolinas Chapter


Over 120 leaders from banking, law enforcement, government and financial services gathered in Charlotte, North Carolina for the launch of the Association of Certified Anti-Money Laundering Specialists (ACAMS) Carolinas chapter. The launch, the largest in ACAMS history, reflected the growing stature of the Carolinas as a national financial center.

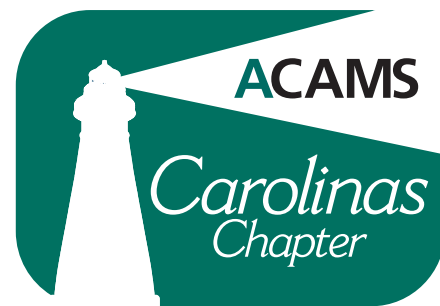
Founding chapter co-chair, William Fox, Global Anti-Money Laundering and Economic Sanctions Executive – Bank of America served as the evening's host. During his opening remarks Fox reminded the audience that "ACAMS is unique because it does not seek to promote any particular industry or influence legislation, but rather seeks to assist the AML professional, whether the professional is in the private sector, the regulatory or law enforcement community, equipping them through training and networking opportunities to excel in their chosen field."

The night featured two guest speakers. First, Les Joseph, Principal Deputy Chief,

Department of Justice, Asset Forfeiture Money Laundering section provided the audience a national AML case update and overview of DOJ's National Anti-Money Laundering Strategy. Les was followed by Jim Candelmo, Senior Compliance Director, GMAC (former Deputy Criminal Chief National Security, US Attorney's Office), who presented on AML criminal investigations and the opportunities for ACAMS members to benefit their organizations by effective cooperation.

John Byrne, former chair of the ACAMS advisory board, closed the program by underscoring the importance of ACAMS chapters, "It is wonderful to see the amazing turnout of professionals from throughout the AML community for this important chapter launch. Vibrant chapters, with meaningful training like we heard here tonight, are essential in fulfilling the ACAMS mission."

By all accounts the night was a great beginning, for what promises to be another successful ACAMS chapter. 



For more information on the ACAMS Carolinas Chapter please contact Jennifer Blake, chapter co-chair, at jblake33@hotmail.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

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

Southern California Chapter

After a very successful launch in September, the ACAMS Southern California Chapter kicked off the New Year on January 20, 2010, with its first learning event titled "A Look Inside the FBI." The event was held at the Boy Scouts of America facility in Los Angeles, California and featured a guest speaker from the FBI's Anti-Terrorism Financing Squad. Despite unusual heavy rains and flooding in the Los Angeles basin, the event attracted a strong turnout of more than 85 attendees.


The FBI presented on money laundering investigations involving terrorism financing, trade-based laundering and narco-terrorism laundering. Specifically, during the two-hour presentation, the FBI addressed their intelligence and investigative roles in counterterrorism, examples of terrorist attacks overseas and how they were investigated locally and abroad from a financial and material support perspective, and how terrorist financiers take

advantage of criminal enterprises and money laundering.

Moreover, local case studies of terrorism financing and money laundering were dissected to highlight the value of information contained in Suspicious Activity Reports (SARs). Further discussion centered on effectively working with law enforcement and the active role of the private sector in BSA/CFT.

The next event for the Chapter will be a diverse panel discussion on Money Service Businesses (MSBs) and is scheduled for March 24, 2010 in Anaheim, California. The discussion shall include a legal and compliance perspective on MSBs, MSB enforcement actions, MSBs and their importance in Southern California, and characteristics of MSBs with successful banking relationships in the region. Similar to the FBI event, this event will earn two CAMS credits for ACAMS members.

The Chapter is committed to continuing to host local and affordable learning events that will serve the diverse financial landscape of Southern California. To assist in Chapter growth, we are currently seeking members to become part of a Task Force that will focus on event and network planning, topic creation, and increasing awareness and membership in Southern California.

In addition, from time to time, the Chapter will host Know Your Chapter Members (KYCM) social and networking get togethers for the community to share ideas, local BSA trends, and meet new colleagues in an informal setting. If you are interested in joining the task force or becoming a Chapter member, please contact us at ACAMS.SoCal@gmail.com. Also, connect with us and stay informed on local news, job opportunities, and events via LinkedIn groups at ACAMS Southern California Chapter. 

Australasian Chapter

The Australasian Chapter has been very active in the latter part of 2009 providing Chapter members with numerous informative events tailored to the Australasian region. As the AML/CTF regime in Australia beds down and the new regime in New Zealand commences these events are a significant resource to Chapter members.

ACAMS endorsed and participated as an exhibitor at the AFMA AML/CTF Conference on November 16-17, 2009. Members who attended heard from local and international subject matter experts on the theme of “2009, Beyond the Storm.” Gregory J. Calpakis, then executive director, ACAMS, made the trip to Sydney to attend the conference and, along with Aub Chapman (co-chair), to meet with John Schmidt, CEO, AUSTRAC.

On November 19, 2009 an event was held in Auckland. The event coincided with the passing of the New Zealand Anti-Money Laundering and Counter Financing of Terrorism Act, 2009. Aub Chapman and Gregory Calpakis were the guest speakers on the topics of “What can New Zealand learn from Australia in AML/CTF Implementation” and “Global AML/CTF trends” respectively. Over the next few days Aub and Gregory had a number of meetings in Auckland and Wellington with universities, industry and government agencies. The profile of ACAMS in NZ has been significantly raised with a number of new members and considerable interest in CAMS certification.

Pre-Christmas networking events were



held in early December in both Melbourne and Sydney. Over 40 ACAMS Chapter members and guests attended in the two cities enjoying discussion on the AML/CTF year ahead.


On December 15, 2009 the first Australasian specific webinar took place. Amanda Wood, General Manager – Supervision, AUSTRAC gave an excellent presentation on AUSTRAC’s supervisory policy. Over 120 participants heard Amanda discuss topics including; reporting triggers; AUSTRAC data mining and data analysis; and

transaction reporting.

Planning for our Webinar program for the first half of 2010 is well advanced with webinars to be held in February, April and June. The February webinar focused on Sanctions, whilst the April webinar is entitled “Implementing the AML/CFT Act, 2009 in New Zealand” and will be our first foray into examining the new AML/CTF regime in New Zealand. The June webinar should be of interest to many and is entitled “Dealing with issues arising in your AML/CTF Program.” Seminars and member events will be held in Melbourne, Sydney, Auckland and Wellington. Members will be informed as to the final dates and topics by email and details will be available on the Chapter web site.

The board has seen several changes in the past few months. We would like to thank those retiring from the board for their contribution in helping the Australasian Chapter grow. So thank you Joy Geary and Arun Kiezpadathil. The board is very pleased to announce that Guy Boyd, AMLCO of ANZ Group, has taken up the position of co-chair.

Guy brings a wealth of experience from one of the Asia Pacific region’s major banking groups.

Our Chapter webpage can be accessed via the ACAMS web site. The Australasian webpage is a dedicated resource for both Australian and New Zealand practitioners. As well as links to regulators’ and legislative web sites, the webpage provides details of Australasian webinars, members’ events and board members. 

ACAMS South Florida Chapter enters its second year and welcomes new Board



As many of you will know, the inaugural gathering of the South Florida Chapter was held in January 2008. Today, after another successful year, we are saluting the dedication of the 2009 executive board who have completed their tenure: Lorenzo Delzoppo, Richard J. Xiques, Johana Ugas, Daniel Foodman, Edson Briggs, Patricia Marinho, Karen Benson, Catalina Rey, Bobbi C Aravuori, Albert Rodriguez, Carlos Gonzalez and Avelino Rodrigues. About 60 percent of the board will remain active to insure continuity of our chapter operations and goals.


The events of 2009 consisted of an inaugural ceremony; three learning sessions:

The Fight Against Mortgage Lending Fraud: What Lenders Should Know, Lessons Learned from Recent FINRA Enforcement Actions, and Anatomy of a Check Cashing Store Investigation; several networking events including our Chapter Holiday Party; as well as chapter members presence at the International Annual Money Laundering Alert Conference and the ACAMS Annual International Anti-Money Laundering Conference.

Despite the economical challenges encountered in these difficult times, the outgoing board expects an increase in membership for 2010 as the South Florida Chapter is determined to continue building upon the program of members' events

held during 2009 and is developing an outline of the program for 2010. This outline will be refined over the next months to ensure an adequate mix of educational and social/networking events. Remember that most of our training sessions count toward continuing education credits for CAMS certification or recertification.

We welcome all ACAMS members in South Florida to join our Chapter, and invite those in the private and public sectors who have not joined ACAMS to do so. See you at upcoming meetings and events!

For more information on future events or to join the South Florida Chapter, please visit the Chapter's web page at www.acams.org/Chapters/SouthFL.aspx. 

Chicago Chapter

On December 15, 2009, the ACAMS Chicago Chapter sponsored its latest anti-money laundering (AML) workshop titled “BSA/AML Emerging Trends,” featuring guest speakers Vincent J. Danno and Karen M. Hooper, Examiners with the Federal Reserve Bank of Chicago. The event was held within the conference room facilities of the Federal Reserve Bank building located in downtown Chicago, Illinois. Attendees included Chapter members and guests from a number of Chicago’s regional financial institutions and financial services companies.

Mr. Danno’s presentation covered new BSA/AML trends, suspicious activities and patterns specifically within the brokerage services industry, where the volume and velocity of transacted funds may often call for special due diligence in analysis of suspicious activity. Several cases involving both institutional BSA/AML program weaknesses and examples of possible money laundering activity involving securities were reviewed. In addition, Mr. Danno dedicated a considerable portion of his presentation to a review of complex money laundering schemes such as micro-structuring, “smurfing,” Automated Teller Machine (ATMs) transfers, Colombian peso exchange, and other sophisticated means used by criminal enterprises in their efforts to funnel large sums of cash both domestically as well as globally.

Ms. Hooper’s presentation furthered the review of BSA/AML trends within the brokerage services and banking industries with additional analysis of recent cases involving complex money laundering schemes. Ms. Hooper’s deep familiarity with FINRA requirements and the intricacies of complex financial instruments was highly beneficial in clarifying the methods employed by criminal organizations to channel funds through financial institutions. Most notable was Ms. Hooper’s discussion of threats from “virtual world” money laundering schemes involving the use of internet games, forums, and other online platforms for money laundering

activities. Recent cases involving this new phenomenon were reviewed, resulting in a highly spirited round table discussion with the audience.

According to Chicago Chapter member and workshop attendee Paulina M. Prebe, CAMS, “Attending this Chicago ACAMS Chapter event on BSA/AML emerging trends was very insightful. The three topics that were covered by the speakers — who are examiners with the Federal Reserve Bank of Chicago — were very interesting and informative. By attending this Chapter event, I had the opportunity to learn about these new trends and stay on top of emerging concerns in the anti-money laundering field.”

The Chapter’s January 21, 2010, workshop on “Mortgage Fraud – What you don’t know will hurt you” generated helpful and introspective dialogue during the Q & A portion of the program. Workshop attendee Brandi Wolfinger, CAMS, reflected afterward that “...the information expands our perspective about the enormity of the problem and how it is intertwined with other fraudulent activity, such as identity theft.” Panelists included Michael Forester of CrossCheck Compliance, Shaun Hassett of The LUBRINCO Group, and Ralph Dahm of I.T. Audit Search. The presentation can be found on the Chapter web site.

The February 12, 2010 workshop focused on system validation issues and how financial institutions must independently confirm the integrity and accuracy of system applications that are relied upon for BSA/AML compliance.

Visit the Chapter web site at <http://www.acams.org/Chapters/Chicago.aspx> for the latest updates about future events and a recap of prior workshops.

For questions or further information regarding membership within the ACAMS Chicago

Chapter, please contact Chapter membership director Terri Downey at teri.downey@rsmi.com or the Chapter email box at acamschicagochapter@gmail.com 



New York Chapter

The ACAMS New York Chapter concluded a very successful 2009 with two fourth-quarter learning events, devoted to the securities and insurance industries, topped off by a well-attended and festive holiday party in December.

As reported in the winter edition of *ACAMS Today*, on October 27, executive board member Erika Jemty of Morgan Stanley Smith Barney moderated a panel of experts who addressed "Hot Topics in the Securities Industry". The panel discussed numerous topics spanning from recent enforcement actions against broker-dealers to emerging fraud schemes plaguing the industry. On November 17, executive board member Martin Feuer of Zurich Insurance brought together insurance industry experts who discussed SAR filings, insurance industry "red flags" and Client Due Diligence issues. Both events were attended by more than 120 members, and the presentations were filled with interesting and practical examples of the current challenges and emerging


anti-money laundering issues in these two sectors of the financial services industry.

New York Chapter executive board co-chairs Barry Koch and Vasilios Chrisos were especially pleased with the positive feedback and strong attendance for both events. According to Chrisos, the board members were glad to see that their early goal of providing a diverse menu of topics for the learning events was so successful. Koch added that plans were already under way for several interesting events for 2010, beginning with the learning event scheduled on February 10 which was devoted to the topics of Human Trafficking and Smuggling. Executive board members David Chenkin and Daniel Wager lead a panel comprised of law enforcement, prosecutors and victims' services representatives. The event included case studies and a practical discussion of the issues and their potential impact on financial institutions.

The Chapter hosted a year-end holiday party at The Penn Club in midtown Manhattan which gave members in the

tri-state area an opportunity to re-cap an exciting year for the New York Chapter and discuss topics of interest for 2010. The elegant surroundings (including the beautiful chamber music provided by the da Vinci Ensemble), combined with the friendly and informal mood of the party-goers, created a perfect setting for a lovely celebration, and offering good wishes for the coming year.

The New York Chapter executive board is currently hard at work planning a full schedule of learning events for 2010 and welcomes your feedback. Please send any event ideas directly to the Board at acams-newyorkchapter@gmail.com.

If you are interested in joining the ACAMS New York Chapter, please contact Chapter co-membership director, David Chenkin at dchenkin@zeklaw.com or Kata Martinez at cmartinez@acams.org. Please also feel free to visit our webpage at <http://acams.org/Chapters/NewYork.aspx> for information regarding future events and materials from past events. 



US Chapter Goodbyes and Hellos

Getting an ACAMS Chapter off the ground is a challenge that requires a special group of people to make happen. The U.S. Capital Chapter's founding board of directors has recently lost two members to opportunities outside of the region. To say we were sad to see them go is an understatement.

Bill McCune, our founding Treasurer, has headed west to take a position with the State of Nevada in Carson City. Everyone in the Chapter, and certainly the board, wishes Bill well in his new endeavors. We hope to see him at the ACAMS conference in Las Vegas this fall.

Heather Brown, our indefatigable founding Secretary, is crossing the pond to England to take on a posting for the Department of Defense supporting AFRICOM. Heather has stated that one of her goals is to help organize a European Chapter of ACAMS. If the energy, organizational acumen and people skills Heather displayed while working for the Capital Chapter are any indication, we can be certain she is the best person for that challenging task. Heather's opportunity is definitely the Chapter's loss and we all wish her the very best of luck in her new role.

While we are losing some great people, some equally great people are stepping up to meet the needs of the Chapter. Kevin Anderson, Senior Vice President at Bank of America is our new Treasurer; Dennis Lormel, Managing Director at IPSA-International is our new Co-Treasurer; and Ed Rodriguez, Manager in Forensic Accounting, Anti-Money Laundering and Advisory Services for Watkins Meegan LLC, joins us as Secretary. Given this group's experience and energy, Chapter members can be confident they will add significant value to the work of the board.

One of the strengths of our fledgling Chapter is our Educational Programs. For example, the January Chapter event — an interview with Eileen Mayer, former head of the criminal investigation division of the Internal Revenue Service (IRS) and now in the private sector — had an excellent turnout befitting the speaker and subject matter. Ms. Mayer told the gathering that the IRS hired 7,000 staff in 2009 as part of its commitment to ensuring that the agency will continue pursuing tax evaders, many of whom are laundering money as well. In addition, she discussed the

value in Bank Secrecy Act (BSA) reports; the clear, strong relationship between drug trafficking and terrorism; and movement of illegal monies to the Pacific Rim. Ross Delston of GlobalAML.com and our program director did an excellent job as discussion leader. A special thanks to Winston & Strawn LLP for hosting the event.

The Association of Certified Anti-Money Laundering Specialists (ACAMS) played a key role in the U.S. Department of State's International Visitor Leadership Program in December. As part of the program, U.S. Capital Chapter board members Debra L. Bonosconi, CAMS, and Heather A. Brown, CAMS, led an interactive session with attorneys, accountants and banking and credit union professionals from Russia to discuss ACAMS and the benefits the organization provides its members.

The Leadership Program, part of the World Learning Visitor Exchange Program, was a three-week conference for Russian delegates titled, "Advancement of Capacities for Improving Financial Sector Transparency, Anti-Money Laundering, and Combating the Financing of Terrorism". The program covered general U.S. policy and its priorities for global security in regards to anti-money laundering efforts at the state and local level, U.S. laws and regulations on money laundering, collaboration and relationships between banks, credit unions and other government agencies, money laundering in the U.S., how the financial crisis has

affected U.S. efforts to provide transparency in the financial sector and the methods used to combat money laundering in the U.S.

Delegation members posed questions regarding ACAMS' conferences throughout the world, training opportunities for banking and credit union representatives, what process is involved in obtaining membership to the ACAMS organization and how to obtain a CAMS certification.

The information and expertise provided in programs such as these are drawing more and more people to Chapter events. Other events were just as strong, such as the February event featuring Thomas Fleming, Assistant Director, Regulatory Policy and Programs Division of the Financial Crimes Enforcement Network (FinCEN). Details will be coming in the Capital Chapter article in the next issue of *ACAMS Today*.

The Chapter is not yet a year old and we are already able to provide a strong set of programs and networking opportunities for our members. Our board of directors is at full strength and filled with talent, expertise, energy and a dedication to the success of the Chapter. The Chapter's networking events are attracting more and more people, some of whom come from great distances. That's why a key Chapter goal in 2010 is to significantly grow our membership. We encourage all DC Metro area ACAMS members to drop by one of our events and see for themselves how they can benefit from joining the U.S. Capital Chapter. **A**



Calendar

<i>Date</i>	<i>Location</i>	<i>Title</i>
March 05, 2010	San José, Costa Rica	Seminario intensivo ALD en el marco de la nueva realidad mundial
March 05, 2010	On-line, United States	Web Seminar - Is Your AML Program In Line with Regulatory Expectations?
March 16, 2010	Singapore, Singapore	Corporate Fraud Investigation and Prevention
April 07, 2010	On-line, United States	Web Seminar - Tracing Internet Gambling: Spotting and Blocking Illegal Payments
April 09, 2010	On-line, United States	Web Seminar - Managing the Terrorist Financing Risks of Banking Charitable Organizations
April 12, 2010	Chicago, IL	Staying Ahead of Money Laundering & Terrorist Financing Trends and Typologies
April 13, 2010	On-line, United States	Web Seminar - New Zealand's new AML/CTF regime – What Does It Really Mean For Your Business?
April 15, 2010	New York, NY United States	Enhanced AML/CFT Tools and Techniques
April 16, 2010	New York, NY United States	Securities Industry Spotlight: Fine Tuning Surveillance, Risk Assessments and KYC Processes
April 20, 2010	On-line, United States	Web Seminar - Applying Enhanced Due Diligence to Detect Beneficial Ownership
April 28, 2010	Ontario, Canada	The Canadian Institute's 9th Annual Forum on Anti-Money Laundering
May 07, 2010	On-line, United States	Web Seminar - Developing an Effective Program to Combat Trade Based Money Laundering
May 10, 2010	Chicago, IL United States	Enhanced AML/CFT Tools and Techniques
May 14, 2010	On-line, United States	Web Seminar - Market Manipulation: An AML Perspective for Brokerage Firms
May 17, 2010	New York, NY United States	Adopting a Risk-Based Approach to Beneficial Ownership and OFAC Sanctions Compliance
June 04, 2010	On-line, United States	Web Seminar - A Growing Threat: Money Laundering through Mobile Banking
June 07, 2010	New York, NY United States	Benchmarking Your AML Program: Analyzing Lessons Learned from Recent Enforcement Actions
June 09, 2010	On-line, United States	Web Seminar - Protecting Your Institution From the Money Laundering Risks of Digital Currency
June 15, 2010	On-line, United States	Web Seminar - Tranche 1 Review of Australian Reporting: Are you Achieving Industry Best Practice?
June 22, 2010	On-line, United States	Web Seminar - Regional Focus: The European Union and the Third Directive on Money Laundering – Keys for International Money Laundering Detection

CAMS Preparation Seminars

February 20, 2010	Riyadh, Saudi Arabia	CAMS Examination Preparation Seminar
March 14, 2010	Hollywood, FL United States	CAMS Examination Preparation Seminar
April 26, 2010	Shanghai, China	CAMS Examination Preparation Seminar
May 14, 2010	New York, NY United States	CAMS Examination Preparation Seminar
June 06, 2010	Amsterdam, Netherlands	CAMS Examination Preparation Seminar

Conferences

April 26-28, 2010	Shanghai, China	2nd Annual ACAMS Anti-Money Laundering & Counter-Terrorism Financing Conference - Asia Pacific
June 7-8, 2010	Amsterdam, The Netherlands	6th Annual ACAMS Anti-Money Laundering & Counter-Terrorism Financing Conference - Europe
September 20-22, 2010	Las Vegas, NV United States	ACAMS 9th Annual International Money Laundering Conference

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 executives** who have come out of this economic crisis stronger and more resilient?

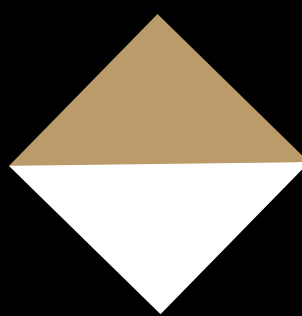
You can. SAS gives you The Power to Know.®

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
for a free special report



THE
POWER
TO KNOW.®



SIGHTSPAN

Navigation for Business Information™

SightSpan MSB Services

SightSpan Inc/ Michael McDonald Associates

WWW.SIGHTSPAN-MSBSERVICES.COM

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