

ACAMS[®] TODAY

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

SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE

*All the world is
real estate 22*



SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE • SHAKESPEARE

SEPTEMBER–NOVEMBER 2012
VOL. 11 NO. 4

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

A tell by any other name 30

PATRIOT OFFICER®

#1 BSA/AML/ATF/FACTA/UAGEA/ANTI-FRAUD

Endorsed By The Largest Bankers Associations and Has Passed Examinations

“THOUSANDS OF TIMES”

Financial
Intelligence
Center



Compliance
Network
UCEN.net



GlobalVision Systems, Inc.

9401 Oakdale Avenue, Chatsworth, CA 91311

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

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

ACAMS[®] 11th Annual

AML & Financial Crime

CONFERENCE

ARIA • LAS VEGAS

Pre-Conference Training: September 30, 2012
Main Conference: October 1–3, 2012

ADOPTING A COMPREHENSIVE APPROACH TO FINANCIAL CRIME PREVENTION

- Private/Public Sector Peer Interaction
- Targeted In-Depth Sessions Presented by
Top Financial Crime Experts
- Practical, Hands-On Training



GOLD SPONSOR

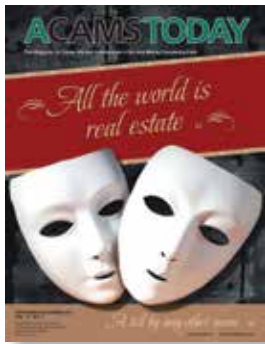


SAVE \$50*

Register and pay by September 21, 2012 with VIP Code AD-50

*Register and pay by September 21, 2012, and save \$50 off the main conference standard price. Pre-conference workshops are not included in main conference pricing. Please be sure to mention VIP code AD-50. Discounted rates are available for government, law enforcement and groups of 3 or more. Please contact Geoffrey Fone at gfone@acams.org or at +1 786.871.3021 for details. Discounts cannot be combined.

ON THE COVER



All the world is
real estate

22

ACAMS Today is designed to provide accurate and authoritative information concerning international money laundering controls and related subjects. In publishing this work, neither the authors nor the association are engaged in rendering legal or other professional services. The services of a competent professional should be sought if such assistance is required. *ACAMS Today* is published four times a year for ACAMS members.

To join, contact: ACAMS
Brickell Bayview Center
80 Southwest 8th Street, Suite 2350
Miami, FL 33130

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

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



ACAMSTODAY

ACAMS

Executive Vice President	John J. Byrne, CAMS
Editor-in-Chief	Karla Monterrosa-Yancey, CAMS
Global Director of Conferences and Training	Eva Bender Williams
Senior Vice President of Business Development	Geoffrey Chunowitz, CAMS
Head of Asia	Hue Dang, CAMS
Director of Operations for Latin America	Gonzalo Vila, CAMS
Director of Marketing	Kourtney McCarty Llopis
Senior Account Executive	David Kehr
Account Executive	Denise Enriquez
Regional Account Manager	Sonia Leon
Regional Manager, Africa, Central Asia, the Middle East	Jose Lewis
Corporate Sponsorship and Advertising	Andrea Winter
Graphic Design	Victoria Racine
Contributing Editor	Debbie Hitzeroth, CAMS
<hr/>	
Chief Executive Officer	Ted Weissberg

ACAMS Advisory Board

Chairman:
Richard A. Small, CAMS
Vice President, Enterprise
Anti-Money Laundering,
Anti-Corruption, Sanctions,
American Express,
New York, NY, USA

Luciano J. Astorga, CAMS
Regional Chief Compliance
Officer, Managua, Nicaragua

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

David Clark, CAMS
Head of Intelligence and
Analysis for Barclays Wealth
Financial Crime, UK

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

William J. Fox
Managing Director,
Bank of America Corporation,
Charlotte, NC, USA

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

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

William D. Langford
Head of Corporate Compliance,
JP Morgan Chase and Co.,
New York, NY, USA

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

**Anthony Luis Rodriguez,
CAMS, CPA**
Global Compliance Officer,
Associated Foreign Exchange,
New York, NY, USA

Nancy Saur, CAMS, FICA
Compliance Manager
Millennium bcp Bank & Trust,
Cayman Islands

Markus E. Schulz
Chief Compliance Officer
Global Life & Banking,
Zurich Insurance Company Ltd,
Zurich, Switzerland

Daniel Soto, CAMS
Chief Compliance Officer,
Ally Financial, Inc.,
Charlotte, NC, USA



- 6 From the editor
- 6 May–July CAMS Graduates
- 8 Member Spotlights
- 9 A message from the executive vice president

10

Dr. Christoph Stückelberger:
The benchmarks of behavior



- 12 The challenges of first generation rules
- 14 The heat is on
- 18 Mobile money

22 All the world is real estate



24 Reengineering compliance strategies
as a counter-crisis measure

28

Revving the innovation engine:
Software as a service for AML and compliance

30

A tell by any other name
–What a poker player can teach you
about recognizing suspicious activity



- 36 Changing the identity management paradigm
- 38 The need for improvement

42

Enhanced due diligence is a must
to mitigate AML exposure in Turkey

46

The AML/CFT enforcement regime in South Africa



48

How banking institutions in Japan should react
to the FATCA Account Identification Regulations

50

動き出したFATCA にどう対応すべきか-口座特定

54

Meet the ACAMS Staff



"All the world's a stage and all the men and women merely players." Words written in England circa 1600 still resonate today. Each person plays many roles in their life. They are professionals, students, mothers, fathers, siblings, criminals and heroes. Shakespeare understood people and the human condition. He understood that regardless of our station mankind deals with the same issues and always has. He was so adept at expressing that understanding that some 400 years later audiences are still enthralled by his words.

You might be wondering what does Shakespeare have in common with anti-money laundering or the fight against financial crimes? Shakespeare was the greatest writer of the English language and as a result if you want to see one of Shakespeare's plays performed today, it is more than likely that there is a Shakespearean production somewhere near you. With that said, we can also agree that a production of financial crimes can also be found somewhere near you.

We all know who Shakespeare was, but many would be surprised to learn that he made most of his fortune not from his art but from business dealings. Like many savvy investors, Shakespeare decided to diversify his investments. He wisely invested in real estate. The famous Globe Theatre was part of what would be termed his investment portfolio. Just as Shakespeare noted in the verse "All the world's a stage," he also wisely showed in his actions that "All the world is real estate."


For the AML professional this idea presents a quandary. It is obvious that real estate, as in Shakespeare's time, remains a tempting target for those seeking to make their fortune. The compliance professional understands the ubiquitous nature of the financial crime and, human nature being what it is, the equally numerous purveyors of said crimes. The quandary is what to do with that knowledge.

The cover article *All the world is real estate*, outlines approaches on how to detect and deter money laundering through real estate. It points out the negative impacts that money laundering has had through real estate on the global economy. Learn what you can do to prevent money laundering through developing a risk-based approach.

The second headline article *A tell by any other name* sticks with our Shakespearean theme. Much like the Bard's famous Romeo and Juliet is studied for its enduring insights, another subject is presented for what it can teach to the compliance professional. All poker players have tells, how one goes about recognizing those tells can be directly applied to identifying suspicious activity in the anti-money laundering/financial crimes field.

This issue of *ACAMS Today* is filled with many more articles to help the compliance professional combat financial crimes. I hope that just like Shakespeare's words still resonate today with many of us, that we as compliance professionals will still find the drive and inspiration to continue with our important mission.

We hope to see you all in Las Vegas at the ACAMS Annual Conference in September!

Also, as always do not forget to send your comments, ideas for articles and submissions directly to me at editor@acams.org. 

Karla Monterrosa-Yancey, CAMS
editor-in-chief

May–July CAMS Graduates

Saber K. Abu Zeid	Shane Brown
Hussein Mohammad Abu-Alim	Jane Budimir
Noor Abu-Maileh	Corina Bulo
Dominic Addeo	Michael B. Burns
Adeleke Aina	Sherie-Claire Butt
Ahmed Akbar	Clayton Byford
Jana Al Hmoud	Jessie ZhuoJian Cai
Ahmed Al Noman Al Shamsi	David Callahan
Jothis Alexander	Brian Carlson
Safwan Suhail Ali Asfour	Christopher Carpenter
Stuart Allan	Cherice Carter
Alecia Allison	Ceazar Castino
Fadi A. N. Aloqod	Christopher Cataldo
Maryam Ambakhutwala	Becky Catanese
Joel Amy	Jane Sandra Cathlin
Mohanan Anandan	Derrick Cerna
Ingrid Aquino	Corey Chamberlain
Sulaiman Michael Aranki	Chau Yen Chan
David Arias Moreno	Paul Chaves
David Artingstall	Yungching (Frank) Chen
Emma Asatoorian	Gary R. Christie
Fahd Athar Ali	Daniel Chu
Mary Audino	Sang Chung
Muhammad Ali Babar	Bryan L. Clark
Zainab A. Bahram	Ian Coffie
Elvia Bain	John Coghlan
Neil D. Baker	Tessie Collins
Arun Balagi S.	Samantha Colomer
Jarrold J. Bang	Lauren Comunale
David Barba	Lisa Cooper
Peter Barden	Rafi Aliya Crockett
Linda Barksdale	Angela Cubbison
Roger Barnes	Krystal Cunningham
Michelle Bashaw	Ahmed Tawfiq Darabseh
Claude Baumgartner	Amirah Darwish
Jummy Rawden Baxter	Teresa L. Davi
Mathew Bedward	Donna Davidek
Nigel Bell	Karin De Jong
Harold Bello	Obdulio De Leon
Kelton Oliver Benjamin	Guillaume de Sampigny
Dana R. Bennett	Francisco Javier Delgado
Brian L. Bernston	Constance E. Denon
Rashmi Berry	Arundhati Deo
Steven Berryman	Sandra Depaoli
Nishanka Bhattacharya	Nikhil Desai
Joe Bimmerle	William DeSantis
Abdul Rahman Bin Bachok	Louis DeStefano
Mike Bingham	Suzanne Detwiler
Marco S. Bodellini	Duncan DeVille
DeAndre Boldon	Yokasta Diaz
Jason T. Bolinski	Macarena Del Pilar Diaz Gomila
Jason Boulrice	Martin Paul Dilly
Colin Bowers	Bryan E. DiMatteo
Mark Bradley	Kelly Dixon
Robert J. Bradley	Jennifer Dombrowski
Margaret Brandon	Sergio Donis
Ishmael Brown	Charles F. Dotter
Margaret Brown	Yannick Douchant
Phyllis Brown	Keith Douglas
Caitlin Brown	Kevin Dreyer



Kacy Drury	Jeannie Guillory	Nishat Lalji	Drew Ryan Nicolls	Rosina Rosales	Chari Turnwald
Abhay Dubey	Aanchal Gulia	Jerome Lamontagne	Brian Nielsen	Elvira M. Rosaria-Statie	Lori Turos
Sarah Dudek	Uday Gulvadi	Lay Lian Shirline Lee	Kamy Niroomand	Petrus Rossouw	Joel Tyler
Jane Dunsmore	Yi Lei Guo	Rebekah Lee	Elizabeth L. Noonan	Catherine Austria Rualo	Athena Tzogas
Lee Ellen Duran	Jen Hall	Fui Zhi Lee	Andrea Nore	Anna M. Rubio	Kenneth Uiselt
Benjamin Duranske	Sara Ali Hani Nouh	Carissa Lee	Juan Novoa	Allison Ryan	Raphael Vaes
Carolyn Durham	Markos Hatzimanolis	Marion Lejeune	Angela O'Brien	Michel N. Salameh	Antonio Valente
Matt Eichenlaub	Lorrie A. Hebson	Rachel Leonard	Margaret O'Malley	April Salathe	Eduward Van De Kamp
Karen Emanuelson	Michael Heider	Kristina Leone	Matthew L. O'Sullivan	Augustine E. Salazar	Alfonso Ventoso
Lucien Emile Barakat	Mavia Henderson	Andrew Li	Sayaka Okoshi	Walid K. Salem	Jonathan Viegas
Vernon Emshoff	Clara Henriquez	May May Liao	Joshua Oliver	Linda L. Sam	Kailash Visht
Bree Ermentrout	Leilanie Herkes	Yanting Lisa Liu	Matthew Olaszewski	Angelica Samudio	John Steven Voit
Candida Etinoff	Lina Maria Hernandez Aponte	David Lock	Hwi Leng Ong	Lyannette Sanchez	Shelly-Ann Walker
Juan Pablo Falcon	Arthur Herold	Angelo Longley	Benjamin Ostrom	Steve Sanders	Hao Wang
Elie Mounir Farah	Steven G. Hickey	Solange Lopez	Helena D. Otto	Hardeep Sandhu	Ava Warner
Rita M. Fares El Khal	Marit Hoegen	Carmen Lopez	Zhi Liang Pang	Petra Sandori	Brittany R. Washington
Parker Fendler	Matthew R. Hollenbeck	Agustin Lopez	Josephine Pank	Andres A. Santander	William Waugh
Christopher Fernandez	Anna Hong	Derek Loutensock	Urvashi Patel	Jack Saunders	Michael Webb
Aaron Baldivia Fernando	Scott Horvath	Andrew MacNeil	Priyank Patel	Sharon Schaefer	Philip Weisman
Micah Ferranti	Julie Hughes	Henry Magram	José Francisco Patiño Ortega	Paul T. Serletti	Alexandria Welch
Brian Ferro	Kyle Hughes	Rakeshkumar Mahangoe	Stephen Paul	Shweta Seshadri	Jeffrey Wentzell
James Filan	Yuqi Hui	Jensy Maier	Michelle Maire Pelletier	Natalya Shafranov	Sharon Werner
Katie Finnerty	Julie Hunter	Shruti Maini	Matthew R. Peppercorn	Sagar Shah	Heather Wester
Maria Cristina Fiorito	Gary Hyde	Karen Malek	Anthony Perez	Chet Shah	Douglas Wiatrowski
Marie Fitzgerald	Yoshihide Ishii	Erick M. Malette	Evelina Pernicheva	Shajuddin Shahid	Alan Wickizer
Kevin Fitzpatrick	Mamoun Mousa Issa	Valerie Manning	Sarabeth Perry	Ranjana Sharma	Robert Widmann
Wayne J. Flavien	Kimberly Jabri	Fouad Marhoum	Mary Pesch	Oleksandr Shchybun	Stuart Wightman
Cathy Fletcher	Christopher Janes	Christopher Martinelli	Titania Peterson-Phelipa	Lu Qi (Cindy) Shen	Christine Wilcox
Jeffrey K. Fletcher	Jeremy M. Janik	Rady Martinez	Maresh Hariharan Pillai	Kien Boon Siew	Martin Wilding
Roderick Flocker	Heba Jaradat	Rosetta Martis	Anastassia Plitman	Kevin Simeoli	Jill Williams
Keyauna D. Forest	Travis Jarae	Nicole Matar	Vasudevan Pondicherry	Melissa R. Sims	Vanessa Williams
John R. Forster	Marjolaine Jardinier	Andres Mayorga	Susan Pouget	Ravindra Singh	Chevala Wilson
Theresa Foster	Vijjayanthi Jayawickama Don	Michael McCabe	Melissa Powers-DePauw	Goran Sirovec	Jeffrey Wingfield
Omar Sharife Francis	Maysa John	Robert W. McCorkle	Laura Pratt Chapman	Sean J. Smith	Randall Witman
Kenn Frantz	Rodney Johnson	Dennis McCreight	Susan S. Pressler	Abraham G. Smith	Stephen Wong
Michelle Frazier	Robert Jones	Sean V. McGlynn	Kristin Pullar	Erin Solovy	Bryan Wong
Michael G. Gallagher	Ryan Jones	Carlos Rubén Mejia	Giana A.S. Quant-Martiena	Kamal Panesar Sood	Anne Woodbury
David Ganger	Galen Kaback	Debra Melendez	Mostafa Qubbaj	Hussam Hoissien Speih	Jinzi Wu
Carla Patricia Garelli Pangrazio	Catherine Kabadian	Kisha Merrell	Camilo Enrique Quintana Alarco	Debbie Sproull	Fangzhou Xu
Paulina Garzón	Carol M. Kaliscik	Kara Meszda	Doris Quintero	Roxanne Stavig	Erin Yang
Kenneth Gaye	Tiffany M. Kam	Elitza Mihaylova	Christian Racine	Edith Steel	Lana Yang
Heather A. Geddie	Ryan Kane	Aleema Mohammed	Sathyamurthy Ramanujam	Robin Stevens	Zhen Yao
Edward Gelfond	Al-Karim Kassam	Priya Mohan	Edmundo Ramirez	Matthew Stewart	Rubina Yasmeen
Ayana George	Talvinder Kaur	Didi Molano	Melvin S. Rapini	Danielle Sugden	Norman T. Yee
Marie-Jose Georges Samneh	Ziad Y. Kazak	Sasha Monyamane	Christina Rasch	Suneesh Sulaiman	Qing Yin
Jeanette Geraldine-Solagnier	Jennifer Kelleher	Deborah Morrisey	Nicholas Ravelingeen	Swaminathan Suresh	Robin Yip
David Gerhart	Elizabeth Kelsey	Necordia V. Morrison	Nilufer Razaki	Karin Tanaka	Chui Ying (Tracy) Yip
Matthew Germond	Jonathan Kessack	Reine Farid Moubayed Moubayed	Brady Rector	Melina H. Tapiz	Yaron Yochai
Joyce Ghaziri Farah	Wasif H. Khan	Tracy Muetze	Mark Reed	Kelly Thomas	Naiping Yu
Silvinder Gill	Jeffrey K. Kim	Albert Mugnolo	William Reger	Stephanie Thomson	Eric B. Zeichner
Judith Gillmore	Dana Klinger	James Mullahy	Rochelle Rego	Monica Tien	Annie Zheng
Nataliya Ginkul	Kevin Klundt	Govind Padmanabhan Nair	Ebad Ur Rehman	Saurabh Tiwari	Xuehui Zhuang
Lauren Girard	Alan Knox	Michael Nam	Daniel P. Reilly	Santiekirian Toewar	Melanie Zimmermann
Lori L. Gleason	Rimmi Kohli	Youmna Nassif	Paru Rellan	Diem Tran	Jennifer Zingel
Prashant Goel	Steven J. Koopal	Khaled Jamel Nassraween	Antonio Phillip Riggio	Daniella Trinchet	Zahid Zoebhai Kalolwala
Melissa Gohs	Ashley Koroluk	Javier Navarro Rodríguez	Joshua Riley	Anthony Troisi	
Carlos Alberto Gonzalez Orozco	Nicholas Kousiaris	Erum Nazir	Lori B. Roberts	Loucas Tsiartas	
Krista Griffith	Polina Kropacheva	Karl Netten	Jarrett Roberts	Sammy Tsui	
Arturas Grigonis	Jonathan E. Kutner	Pei Wen (Natalie) Ng	Emma Robinson	Shweta Tulsyan	
Nicole Guiffra	Michaela Kyle	Wai Yan Ng	Sebastian Roca	Brian Turner	



Henri Faizi Auni
Democratic Republic of Congo

Henri Faizi Auni is vice president of CENAREF, Financial Intelligence Unit, in Democratic Republic of Congo.

Faizi has been engaged in AML since 2003 as chair of GREB, Working Group against money laundering and terrorist financing set up at Central Bank of Congo. He was fully and actively involved in the creation of CENAREF in 2009 and has participated in numerous international conferences (FATF) and seminars (Egmont Group). He also visited several times the Belgian (CTIF) and French (TRACFIN) financial units for training. He chaired national AML conferences for banking and mining sectors, accountants, lawyers and other executives of law enforcement units with financial support of IMF and World Bank.

Faizi has 10 years of experience in the banking sector as head of Bank Supervision Department at Central Bank of Congo and manager at Financial Control Unit at CITI (Congo). Prior to joining CITI he worked for two international audit firms KPMG and PwC and also as an independent financial consultant. He undertook, in high level, both audit, consulting and investigation assignments in his country and other Central African nations such as Republic of Congo (Brazzaville), Cameroon and Burundi.

Faizi graduated from High School of Commerce at Kinshasa in Democratic Republic of Congo and is a member of associations for accounting and audit professions in his country. Faizi is striving with his colleagues, to strengthen CENAREF as an efficient tool in the fight against money laundering, fraud, corruption by using many opportunities offered by ACAMS.



Chris Cuzzucoli, CAMS
San Francisco, California, USA

Chris Cuzzucoli joined Schwab in March 2010 as the AML/OFAC officer for Charles Schwab & Co., Inc., and was later appointed to the same position for Charles Schwab Bank and Charles Schwab Global Services, a money services business. He is also the officer responsible for Schwab's Anti-Bribery program.

Cuzzucoli's career has included positions in the legal, compliance, operational and risk management areas of AML. Prior to joining Schwab, Cuzzucoli served as North American head of AML for Barclays Corporate Bank, and previously served in the same capacity for TD Bank USA/TD Ameritrade and Dresdner Kleinwort Wasserstein/Dresdner Bank. While at Citi, he served in various roles, including global head of AML and global head of Account Intelligence Units for Global Transaction Services, and as AML counsel for Salomon Smith Barney.

Cuzzucoli started his career on Wall Street working on securities litigation and has 17 years of experience in banking and securities. He is a member of the Bar in New York, Colorado and Washington, DC, is a Certified Anti-Money Laundering Specialist (CAMS), and has presented at AML conferences in Africa, Asia, Europe and the Caribbean. Cuzzucoli is a member of the Securities Industry and Financial Markets Association (SIFMA) AML Committee, served on the 2011 ACAMS Conference Task Force and as the co-chair of the 2012 ACAMS Conference Task Force.



Lisa Kelaart-Courtney, CAMS
Dubai, United Arab Emirates

A dedicated governance, risk and compliance professional with both a practitioner and regulatory background, Lisa Kelaart-Courtney leads the Compliance Advisory Services division of Clyde & Co LLP, an international law firm with offices globally. Kelaart-Courtney and her team provide governance, compliance and risk consulting and advisory services and solutions in the GCC region, with a predominant focus on aspects of financial crime including AML and CFT. She has many years of experience supervising and implementing compliance, risk and governance programs for corporate entities and regional regulators in the Middle East, North Africa and Asia.

Prior to joining Clyde & Co, Kelaart-Courtney held senior roles including technical advisor for the International Monetary Fund (IMF), where she served as an expert on a range of projects pertaining mainly to financial crime.

In addition, Kelaart-Courtney held the post of associate director in supervision with the Dubai Financial Services Authority

(DFSA). She was the DFSA representative to a number of international standard setting bodies, held membership positions on technical committees including those relating to fraud and financial crime and was a contributing author on international guidance papers about money laundering. Kelaart-Courtney also represented the DFSA at the AML/CFT standard setting body, the Financial Action Task Force (FATF) and participated in the FATF Typologies Project which focused on reviewing AML regimes.

Kelaart-Courtney underpins her professional experience with professional qualifications including and not limited to Masters of Commercial Law; double MBA and holds certified qualifications as a Financial Analyst; Risk Analyst; Certified Anti-Money Laundering Specialist (CAMS) and Fraud Examiner.




Pieter Rossouw, CAMS
Pretoria, South Africa

Pieter Rossouw has a LL.M. in Criminal law, and had a distinguished career as a public prosecutor and a military law officer. As such he was involved in the investigation and prosecution of a number of serious and complex criminal matters as well as internal irregularities. As a military law officer Rossouw was appointed office chief of several regional offices and not only successfully managed all aspects of a multi-disciplinary office, but was also responsible for management of regulatory compliance and stakeholder relationships.

After leaving the defense force with the rank of Colonel, he entered private law practice as an advocate for a number of years.

Driven by a passion for excellence and commitment to the fight against crime and corruption, Rossouw started off on a new journey two years ago to transform himself from a lawyer into an Anti-Money Laundering Specialist. In this process he obtained a post graduate Certificate in Money Laundering Control (cum laude), passed his Financial Services Board Regulatory exam with 94 percent and his CAMS certification exam with 96 percent.

He is involved in the ACAMS mentoring program, and is currently looking forward to new opportunities in the AML environment. 



We can all do better —ACAMS can help

In the United States, we are in the midst of a presidential election year and many are bemoaning the lack of civility in public discourse. With all of the many avenues of communication (“including those known as social media”) it seems that competing (and sometimes supporting) interests are unable to rationally discuss major issues of the day. A book I am currently reading, *We Can All Do Better* by former U.S. Senator Bill Bradley, stresses the importance of finding wisdom from individuals from all walks of life. In our world, that means compliance professionals, analysts, lawyers or auditors can all provide valuable insight on the issues we need to address.

Mr. Bradley (also a former sports star in basketball) points out toward the end of his book that “the time for cooperation has arrived.” While his issues are public policy discussions in the legislative branch and political campaigns, it seems to me that this can easily be applied to the expected changes in AML that will result from the recent report and hearing in the United States on HSBC. Cooperation among the private sector, law enforcement, regulators and policy officials remains essential to a successful response against financial crime.

Those of us who have been engaged in the money laundering prevention community know that when a major report or enforcement action is leveled against a financial institution, the entire industry can be impacted. Whether it is in the form of

increased regulation, new laws, guidance or simply increased and aggressive regulatory oversight, the AML community needs to sit up and take notice.

The HSBC case study goes far beyond an individual institution and the recommendations by the Committee releasing the study covers all related products or services that in the view of the Committee present increased vulnerabilities for money laundering and financial crime.

ACAMS held a free webinar for our members in July to cover these recommendations, and it seems to me, that unless there is strong and open communication between the private and public sectors, we are doomed to failure.

The report criticized the government for some failures to act, and the bank (and of course our institutions that offered similar products) for several oversight deficiencies. All of these issues can impact future AML and related examinations and all financial institutions. I believe it is up to us at ACAMS to provide forums, programs and communication vehicles to assist the AML community as they grapple with all of these challenges. We will provide that help.

Specifically, the Senate Committee recommended, among other things that:

- Banks close accounts with links (or suspected links) to terrorist financing;
- Boost information sharing among affiliates (a directive made difficult with competing and conflicting jurisdictional requirements);

- Increase AML resources—a direction to be smart about tools and training; and
- Directing the agencies to strengthen AML examinations—a point that will undoubtedly result in more fines, penalties and formal criticisms for years to come.

There were many more recommendations so I encourage all of you, here in the United States and throughout the world, to read this report, which can be found at <http://www.hsgac.senate.gov/subcommittees/investigations/hearings/us-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history>.

ACAMS takes our responsibility seriously to stay abreast of actual and potential changes in the AML community, wherever it may occur, through production of articles in *ACAMS Today*, [ACAMS moneylaundering.com](http://ACAMS.moneylaundering.com), our plethora of educational offerings and our new products lines of advanced certification and the ACAMS Risk Assessment Tool.

Whether it is oversight within an institution by the compliance professional or outside by external auditors or regulatory overseers, we can all do better. Cooperation is the key and ACAMS is honored to host any event where those discussions can take place. **A**

John J. Byrne, CAMS
executive vice president

SARSnSTRIPS



Produced by ComplianceComm



Dr. Christoph Stückelberger: The benchmarks of behavior

A CAMS Today had the opportunity to chat with Dr. Christoph Stückelberger, executive director and founder of Globethics.net Foundation in Geneva, Switzerland.

Stückelberger is also the professor of Ethics at the University of Basel, Switzerland and has a Ph.D. in theological ethics (peace ethics) and habilitation in environmental ethics. He was the founder (1995) and first president of Transparency International Switzerland and for 15 years he was the director of the development organization "Bread for all." He has published hundreds of articles and dozens of books on ethics, among others on corruption such as "Corruption-free Churches are possible" (2010).

ACAMS Today: Why did you choose to study ethics?

Dr. Christoph Stückelberger: Ethics is a way to find an answer to the question what is good and what is bad? Ethics is also a way to find criteria in a fast moving world where former, ancient moral norms are often not giving an appropriate answer to current challenges. I also wanted to be more precise in developing the methodology and scientific approach, with the practical goal of implementing justice, transparency and freedom in the different sectors of society.

In addition, I was also studying theology so I studied ethics from a philosophical and theological standpoint. The question for me was how to implement Christian faith and values in the modern globalized world and

in personal life in a responsible, transparent and inclusive way. In the end that was my motivation.

AT: In brief what is applied ethics?

CS: Fundamental ethics is the methodology of what are the basic values such as peace, sustainability, participation and justice. Applied ethics tries to apply these fundamental values to specific fields or questions. For example: "How to implement transparency in financial transactions?" or "How to manage a company based on honesty and responsibility?" these are questions of applied ethics. This is how ethics is applied to specific activities either professional, family or community life or law.

Ethics is something that deals with all aspects of life, not just with human resources, social or philanthropic activities. Each decision includes an ethical question because one has to decide between two or more options. What are the reasons or values behind deciding between one option or the other option? A crucial conflict is between a decision for personal benefit or for public interest. You can make a decision where you decide to defend the public interest even if this ethical decision has personal cost e.g., for your career.

AT: What led to the founding of Globethics.net?

CS: Globethics.net is based on three pillars: Development through *access* to information, ethics through the sharing of values as a *network* and the importance of *online* communication in a globalized world.

Development through access of information: Through my experience in working with many developing countries I noticed the limitation of access to information that many people have. The desire for these countries to have access to digital information is what led me to launch Globethics.net. Globethics.net provides the leading digital ethics library to everyone free of charge.

Ethics through the sharing of values: In an international-globalized world we need the interaction between value systems, between different world views and religions. Each of us has our own values, but in order to interact with each other we need to find common ground (global ethics) between the value systems. This is something AML professionals deal with on a daily basis because they are dealing with an international financial system.

Importance of online communication (internet): The goal of founding globethics.net was to position it as a global online network, to access information and sharing of values. Globethics.net is a growing community with over 60,000 registered participants from over 200 countries. The membership is comprised of specialists from different business and political sectors. Registered members have access to over one million documents online. Registration is free.

AT: What are the largest ethical challenges facing the global marketplace?

CS: 1) On a macro-economic level, the largest ethical challenge today is how to regulate the financial markets in a way that they serve the real economy by implementing stronger legal mechanisms, regulations and reducing

purely speculative transactions. AML specialists help strengthen the financial-transaction control by implementing the financial laws.

2) On an individual level, the average person in many countries tends to live in a world that is corrupt. Many people therefore say if my neighbor can get away with it why shouldn't I do it. As a result corruption is still increasing despite the efforts of companies, governments and civil society to mitigate corruption. There are manifold individual and structural reasons for this as I explain in my books on corruption (e.g., "Corruption-free Churches are Possible," download for free from www.globethics.net, library).

AT: What ethical challenges should AML professionals be mindful of in the course of their daily activities?

CS: I have a high respect for AML professionals because they play an important role in reminding a company, professionals, the public sector and society of their obligation of honesty, transparency and for fair play in business and financial transactions. Ethical challenges are complex. For example, how to trust in society and in business transactions. If there is no trust, we need all sorts of control mechanisms, leading to more controls, and in the end we are over controlled and still do not find healthy business transactions because trust is missing.

How to balance trust and control is an ethical challenge. We need control and AML professionals have a noble and important task in controlling as closely and as detailed as possible, but we also need the balance of trust in other people and not to see a criminal behind each person. This leads us to individual ethics and structural ethics. Individual ethics would call on the individual and appeal to them to behave in a good way. Structural ethics is more to prevent — by laws, sanctions, organizational measures media pressure — an individual from doing wrong or doing evil and to stop destroying others through criminal activities. Both are needed as a means to strengthen the legal framework and to have strong sanction mechanisms, but on the other hand we also need the individual's responsibility and consciousness. So how can the legal system help the individual not solely rely on the letter of the law by saying well I have complied with the law so I am

fine. Behind each law the individual also has their professional and individual responsibility. Even if the law allows something within reason, if my values tell me it is not right to do it we shouldn't do it.

Also, AML professionals can't only deal with AML issues in a technical way; it is a form of art because you need a deep understanding of human behavior. For example, what are the drivers of criminal mechanisms in society? This makes it fascinating and there is a lot of ethics involved. Ethics requires, at the end of the day, a profound understanding of human behavior, weaknesses and how

Ethics allows us to
reflect on the values
that we defend

we deal with temptations. Many criminal activities come about because of temptation or peer pressure. Criminals see an opportunity to satisfy their greed and addiction. So the question is how to deal with addiction, greed and dependency from peers? People who have this addiction are not controlling themselves.

AT: How can an increased knowledge of ethics be a benefit to the AML professionals?

CS: One of the key elements that ethics can contribute is to show the benchmarks of behavior. To remind ourselves and society what are the basic values we need to maintain; for example, fairness, same fundamental rights, freedom of decision, mutual respect for the dignity of all human and non-human beings. Ethics allows us to reflect on the values that we defend. AML is an instrument for a more fair and transparent society.

You can get concrete instruments from ethics on how to make decisions. For example, how to deal with dilemma? Some people are helpless when dealing with dilemma because a dilemma means you have to decide between two good solutions or two bad solutions. How can you decide which is the better of the two bad options? Ethics can help by framing it in a way to know that one is not perfect but accepting the fact that one has a dilemma and is trying their best to base their decision on their values — it is a moral compass. Ethics should not just create bad conscience but should also offer relief and release. We can mutually encourage each other to be faithful to our professional values.

Also, after my keynote address at the ACAMS conference in Amsterdam, many compliance professionals came and told me that they now see their AML activities in a broader perspective and how it is meaningful for society and what are the key values we have and can defend. The strength of AML professionals is that they have the knowledge of new technical and legal developments; however, one of the dangers with having these strengths is that AML professionals may be too technically detailed. What is all that about? It is necessary for AML professionals to find a balance by stepping back and looking at what they are doing. Ethics can motivate and orient professional activities and help them keep the vision of a just and open society. AML professionals often deal with the negative, criminal energies in society, but it is important to remember that there are also a lot of positive energies in society by resisting and overcoming destructive tendencies. If law and ethics complement each other and if ACAMS and Globethics.net cooperate, both sides will be strengthened in their services for a more humane and fair society. **▲**

Globethics.net Foundation is a global ethics network based in Geneva with a global leading online library on ethics (one million full text documents) and over 60,000 registered participants from 200 countries. A cooperation agreement between Globethics.net and ACAMS is in preparation.

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

The challenges of first generation rules

Rules or detection scenarios are at the heart of an anti-money laundering (AML) software solution. It is through rules and profiling that a compliance group is alerted to suspicious activity. Yet many systems rely on rules that were developed over 10 years ago. These first generation rules present a number of significant challenges to the chief compliance officer (CCO). At the same time, regulators are increasingly focused on the appropriateness and effectiveness of the rules employed together with the CCO's ability to justify the way in which rules have been implemented.

Clearly a better approach must be followed. Fortunately, most systems allow for the creation of new and customized rules. With this flexibility a financial institution can overcome the limitations of the first generation. The following are some of the key challenges. Addressing these challenges will significantly improve the effectiveness of the compliance function.

Challenges

AML detection rules present a number of challenges to the CCO. These challenges can be broadly classified into five major areas:

- Fundamentals
- Logic Issues
- Control Issues
- Case Management Issues
- Poor Supporting Information

Fundamentals

Rules-based detection systems are fundamentally flawed if they are not driven by a risk-based approach. Rules should be chosen by and thresholds adjusted based on a systemic risk assessment inherent in the AML software. Further, both rules and the risk assessment should be dynamically and continuously adjusted based on the prior

actions, behavior, and transactional patterns encountered. It is only through a true feedback loop between detection and risk assessment that a system can stay relevant through ongoing business change.

Logic issues

This is the most significant challenge facing CCOs. Is the logic used by each rule sufficiently robust to detect true suspicious activity? From our engagements with a wide range of clients, it is clear that the answer to this question is often negative.

More troubling is the fact that many CCOs do not have a way to assess the validity of their rules. Vendors often provide rules as a "black box." The logic and details are not exposed or explained. The CCO is faced with the problem of "not being able to check what has not been found." This leaves the financial institution at significant risk. Rules designed a decade ago are used for many years without any reasonable way to assess their competence. Consequently, true suspicious activity is often undetected.

Three of the most common logic issues are:

1. *Weak Logic:* The algorithms used in many first generation systems are very basic and do not adequately detect suspicious activity, especially new or emerging patterns. Often these algorithms use a simple query rather than employing other approaches such as statistical, pattern detection, and trending. To help determine the adequacy of rule logic, the CCO should ask their vendors to explain the approach used for key detection scenarios and provide a justification for their approach.
2. *Excessive False Positives:* A corollary of the weak logic used in many detection scenarios is an excessive number of false positives. Generic rules often cast a wide net creating unnecessary alerts and cases. The substantial effort and

cost of resolving these cases is troubling enough. Yet, one must wonder, how many valid cases are not properly researched because the finite resources available to the CCO are diverted toward useless alerts. It is not satisfactory to say that large numbers of false positives are a byproduct of AML compliance. They can be reduced while maintaining adequate safeguards.

3. *Number of Rules:* AML vendors will often create a large number of rules to demonstrate the competency of their software products. On the surface, this may seem like a good approach. However, it is often problematic. The logic for detecting suspicious activity should take into account all relevant behavior for a particular typology. Designing rules for very specific situations often prevents the rule from using all of the relevant information available in transactions and other data.

Control issues

Detection scenarios must be adapted to the transactional patterns, clients, products, and most importantly the risk of a financial institution. They should not be used as-is from the software vendor. All too often, the only control offered is through a limited number of inconsistent rule parameters and thresholds. For a financial institution to gain better control of their suspicious activity detection, they should have:

- A comprehensive set of parameters and thresholds that are applied to most if not all rules.
- Good guy lists and other exclusions that are rule specific and that can be applied conditionally based on the needs of the financial institution and its specific products and lines of business.



- Comprehensive analytics that provide a deep understanding of transaction patterns and the reason alerts are, and more importantly are not, generated.
- Control over the creation of alerts and cases to properly represent the nature of the finding.

Case management issues

A comprehensive case management and research facility is essential to efficiently and effectively handle suspicious activity alerts. At the rule level, case management is hindered by the following scenarios:

- *Alert Overlap:* The large number of rules offered by AML system vendors often overlap in the type of activity they are monitoring. As a consequence, multiple cases are created with each providing only partial transactional details. This creates extra work for the compliance group and hampers the ability to view all suspicious behavior holistically.
- *Cases by Rule Instead of Party:* Related to alert overlap is the segregation of cases by rule instead of by the suspicious party. Suspicious activity is inherently party centric and should be viewed as

such. Complete supporting information, analytics, and past cases should support the review of all suspicious activity for each party.

- *Creation of Cases Instead of Alerts:* Here I will be specific with terminology. An alert is simply an indication that some transactional pattern should be looked at. A case is the promotion of an alert based on an initial evaluation that suggests that detailed and further research is warranted. The challenge with some of today's systems is that rules such as profiling will automatically create a case instead of an alert. This substantially increases the burden and risk for the CCO since regulators will look for cases to have more due diligence applied even though many may represent false matches.
- *Dynamic Learning Unavailable:* Today's systems must employ dynamic learning to meet the needs of compliance. A static model that is programmed once is not sufficient. Systems must capture all of the information inherent in research and case management. This information must in turn be saved and influence the actions followed by subsequent and similar situations.

- *Weak Scoring:* An important tool to help prioritize alerts is a proper scoring methodology. While some systems have implemented scoring, it is often a trivial calculation that does not properly reflect the level of risk inherent in an alert. Scoring methods should be model driven affording the ability to adapt it to the risk profile of the financial institution.

Poor supporting information

It is often said that the results are only as good as the data available. While this is true, it leaves out another important truism. That is the results are only as good as the analysis of the data available. Successful AML systems must now provide true analytics to support the research of cases and to uncover new suspicious activity that may not be found by the existing rule set. However, most systems are limited by basic database queries that are frustrating at best.

To support rules, a fully functional business intelligence capability must be provided. This capability must offer:

- OLAP (online analytical processing, that rapidly provides results of detailed data relationships).
- Statistical modeling to help identify facts and patterns in vast amounts of transactions.
- Visualization tools aimed at simplifying the relationship in data.
- Information capture that provides the ability to save and reuse prior analytics.
- Knowledge consolidation that allows the combining relational, public, corporate, and commercial data.

Conclusion

These challenges are significant and have gone unaddressed for a substantial period of time. This should not continue. Examiners are asking for detailed analyses of what rules have been chosen and why. They are asking the CCO to explain why parameters were specified in the way that they have and how this is supported by existing data and the risk assessment of the organization. Further, they are looking for strong statistical support rather than a simple narrative. The time has come to reassess your rules. **▲**

Salvatore Cangialosi, president, Telavance, Inc, Iselin, New Jersey, USA, sal@telavance.com

The heat is on

New and
revised
pressures
for AML
compliance

Do all of the requirements across global and local authorities make your head spin? They certainly have accumulated over the past ten years. This year alone, the activity level has been high among global policy-making bodies working through new guidance and pending rules. With the recent Financial Action Task Force (FATF) revised recommendations in February, customer due diligence (CDD) has been given a spiffy new suit of clothes via clarified rules.

The identification of beneficial owners and formal listing of high-risk jurisdictions were named as key issues by the FATF in February this year when it updated its recommendations, prompting discussion and preparation for change. Electronic identity verification (eIDV) and watch list filtering for faceless interactions are more relevant than ever. How and where you implement these tools across teams and business lines — not only before, *but after* account opening or initial financial product purchase — will now be under a higher strength microscope than has been experienced in prior years. Watch for clearer expectations for more CDD throughout your organization and harsher consequences if you fall short. Some institutions are already feeling the heat through more detailed audits, harsher penalties and consent orders to which they must respond.

Requirements for strengthened CDD are spreading across the globe

Verifying that a new customer is who they say they are when they phone in to your sales offices, when they log into your web site to access services or an account is not easy, as we all know. It becomes even more complex when you must also verify the hidden owners, or beneficial owners, not readily apparent in your information collection in the client application process and ongoing during the life of the account or financial product ownership.

Constantly evolving financial crimes are compounding the scope of risk management and increasing the need for strengthened CDD and refreshed identity verification (IDV) frameworks and rules. This is a trend with countries as well, which are looking toward a higher degree of CDD and a tightening of IDV rules, the latest being New

Zealand. Advancing risks of corruption and bribery, high-risk jurisdictions and adherence to tightened Office of Foreign Assets Control (OFAC) sanctions programs are a few of the sizzling hot topics in the regulatory landscape. It is important to note that, although employee-related fraud is ever present in all industries worldwide, this article focuses on the customer-centric risks highlighted by authorities that are impacting covered financial institutions by the global anti-money laundering (AML) regulations.

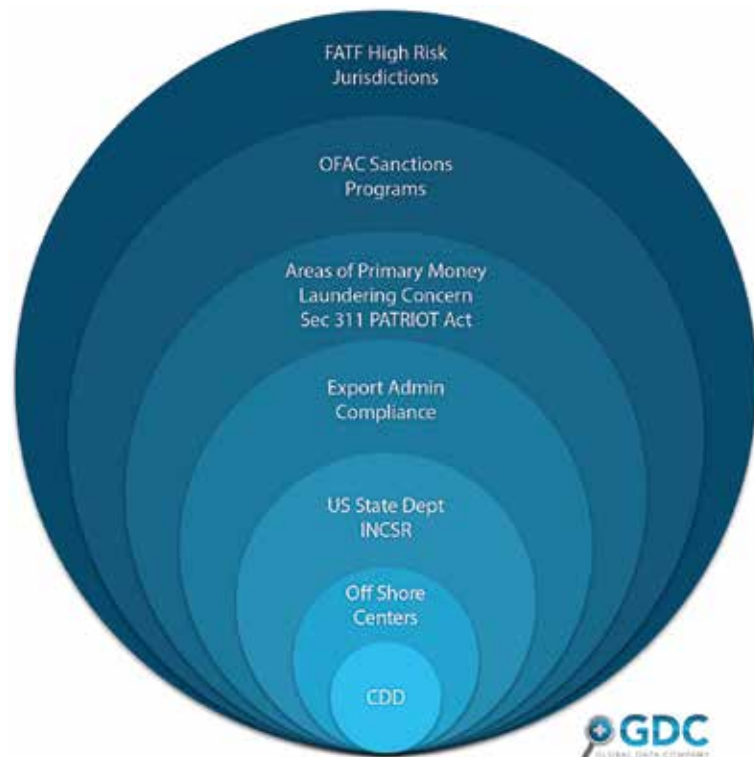
These risks are not new, but the FATF and governments around the world are highlighting new and growing risk elements within them. As a result, a trend of refined IDV and CDD requirements are emerging in pending rules across the globe. Organizations are receiving greater pressure now to more precisely identify their customers and examine their activity. For example, New Zealand has recently included prescriptive



eIDV rules as a key element of their new guidance.¹ Watch for this best practice to become a global trendsetter. Regulators and other overseeing authorities worldwide are looking at how programs and tools or capabilities within are actually functioning and whether they successfully mitigate the vulnerabilities identified in the risk analysis. Many examiners and auditors are now reviewing closely the way a financial institution's eIDV programs and procedures monitor customer activity *throughout* the account's life cycle.

What does this mean for your business? The example in New Zealand shows us that applying more logic and practicality to your verification rules and program will not only meet compliance and prevent risk, but it can save time and money. Simplifying steps while maintaining integrity and quality of the risk management makes sense to your bottom line and requirements. The New Zealand rules simplify the steps to point to a single source of identity data in their rule framework while maintaining security in the

Example of various requirements worldwide for which there are tools to aid compliance.



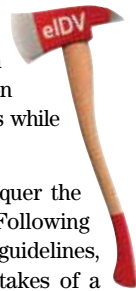
¹ Identity Code of Practice 2011, New Zealand, [http://www.dia.govt.nz/Pubforms.nsf/URL/AML/CFT_IdentityVerificationCodeofPractice2011.pdf/\\$file/AML/CFT_IdentityVerification-CodeofPractice2011.pdf](http://www.dia.govt.nz/Pubforms.nsf/URL/AML/CFT_IdentityVerificationCodeofPractice2011.pdf/$file/AML/CFT_IdentityVerification-CodeofPractice2011.pdf)

verification process, and so can you. Talk with your regulator on how to abide by your regional rules while employing best practices like these.

Flexibility and extra time to conquer the learning curve with AML are over. Following FATF's revised and renewed guidelines, authorities affirm continuing mistakes of a basic nature to be inexcusable and consequences are increasing in severity.

Reinforcing this concern in the globe are consent orders issued by regulators over the last two years. Still present are a volume of basic deficiencies in core AML program components. For example, the failures to adequately identify the actual customer (including all beneficial owners) and appropriately monitor activity are still commonly found violations.²

Even in the busy workplace you should try harder to stay in touch with FATF guidance. Its direction influences policy across the world, after all. The latest revisions are clearly making waves. Keeping up-to-date on the reports by this source, as well as those by your local authority, will help you tighten your CDD program to meet new requirements, prevent common mistakes and avoid costly violations.³



Leveraging existing tools to aid an enterprise-wide client-centric risk profile

Not identifying all beneficial owners of an account or financial product indicates you don't understand with whom you are doing business. As a result, your regulator will view your opportunity to accurately recognize where your risks lie across your organisation as dangerously diminished.

As pending rules around the world are finalized, regulators will be examining institutions in detail for how IDV occurs at service entry and ongoing throughout all access points in the institution from customers and hidden owners after initial account opening. Examiners will review how well you identify risk in customer activity as funds and account activity move across your various business lines and service delivery methods.

Key will be identifying all owners with access and control of the account. Also critical will be your expectations of the transactional behavior, whether you are assessing it ongoing and have controls in place if suspicious activity occurs. The review will inevitably include the controls in place for IDV/eIDV, the watch lists selected to screen customers and beneficial owners, as well as those used to flag high-risk jurisdictions. A deeper drill down on CDD is fully expected. There is good news, however. Meeting the refined requirements need not be so daunting. New guidance has cleared murky waters.

You can leverage existing tools across the high-risk areas of the organisation and meet the new requirements by revisiting your Risk Assessment (RA) with an internal team. Include your regulatory authority in the self-imposed review or invite their input ahead of any formally scheduled exam. Look for all places across the flow of funds where beneficial owners may be acting behind a nominal owner. Identify business lines or units where the most resources, tools and attention are needed, and where the highest risk transactions occur. Apply an enterprise-wide client risk approach to your process (see the figure below left for a definition of this type of approach.)

Get familiar with and apply the new FATF recommendations. Include in your review where new co-owners or beneficiaries are likely to enter again after customer relationships are initially formed. Review the tools and teams in place to ensure they support procedures and controls. Again, invite regulator feedback outside of an exam when you review your program and procedures for the fit with the new and revised CDD rules.

Recommended risk lists

Compliance challenges involving some of the hot topics in the globe mentioned above are most efficiently met with the appropriate watch lists suited to business and your level and type of risk, as well as to your formal requirements. There is an abundance of watch lists in the world for a variety of risks and due diligence needs. Just as your risk depends on your type of business, the kinds of customer target groups you serve, where you are located etc., the watch lists you choose depend on these factors as well. Generally, you will find that authorities will recommend a subset of watch lists for each institution, based on their size, location, target area and other factors that affect their risk. Ask for your regulator's opinion on how to tailor a fit for your risk-based need and for your institution in general. If you are accountable to prescriptive rules in your compliance requirements, your regulator will have advice on lists to fit both your requirements and risk combined.

Watch lists can be very basically divided into two types for ease of understanding; core watch lists (required) and watch lists for enhanced due diligence (EDD). What is a core watch list for one institution may be an optional EDD list for another. There are different types of watch list categories for entities (businesses, individuals, vessels, organisations, and location specific sanctions programs) that are deemed high risk in a variety of regards.

Core watch lists are most often government sourced and individual countries may require one specific to the country that is often derived from the United Nations Consolidated List



Definition of Enterprise-wide Client Risk:

The risk represented across the organisation in a wide variety of detailed information relating to the customer's account — from account opening throughout the account life cycle. This is assessed from a single view of the customer profile, incorporating all of the various financial relationships with which the account has an affiliation.

² The United Kingdom's banking regulator penalized a Zurich-based financial institution in May this year along with its former anti-money laundering officer a combined 540,000 pounds for broad failures in risk-ranking and enhanced due diligence procedures. (Moneylaundering.com, May 22, 2012, <http://moneyjihad.wordpress.com/2012/05/30/habib-bank-throws-caution-to-the-wind/>)
³ Go to FATF's recommendations page. (<http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfrecommendations2012.html>)

(UN Resolution 1267, 1617 etc.) Examples include the OFAC, Australian Department of Foreign Affairs and Trade (DFAT), and European Union Consolidated List.

EDD watch lists are not universally required and may be industry-based or risk-based. These include non-government watch lists, such as the one for the World Bank Ineligible Firms list; the Bureau of Industry and Securities List for export administration compliance; and the Organization for Economic Co-operation and Development (OECD) Uncooperative Tax Havens List.

Your IDV/eIDV and watch list programs, as part of your larger controls and procedures with CDD, can contribute to a significantly improved bottom line through reductions in identity theft, fraud losses, reputation damage and more. If leveraged successfully, existing tools and teams can be realigned and disseminated across the organisation to not only strengthen CDD, but also improve the customer experience and increase revenues. Take a moment below to see how your CDD efforts measure up today to the revised FATF and related guidance for your location.

How do you rate?

In a minute or less see how amenable your organisation is toward a customer-centric approach right now. The steps below are one example of guidance interpretation. You can amend these to suit your interpretation and have your regulator review and comment.

Use this example to see how you rate and how much work you may have left to do to meet the new pending rules.

If you answered “yes” to three or more of these, your organisation may be adaptable to a customer-focused risk model but you still have work to do. If you answered “no” to any one of these, the number of deficiencies found in your federal review will increase along with the amount of remediation required. If you answered “no” to any two or more of these, your chances of violations are high.

Don't get burned by being caught with holes in your understanding and your compliance program.

CDD is an evolving process as your business and markets change. It is time to open up the official reports and rules and get familiar again...and do so regularly. The world is witnessing evolving criminal activity. Tools the criminals are using to commit crime are continually developing too; informal value transfer systems, mobile phone access, expanding realms of the Internet and more. All of these evolutionary changes provide growing opportunities for criminals to hide their identity.

The revised FATF recommendations offer extremely helpful guidance toward addressing these challenges to eIDV in particular. The more targeted risk-based approach in “following the money” will no doubt be challenging, there is no way around that.

Summary of Advice Regarding New & Pending Rules

- Pay attention to the policy formation, enforcement actions and reports. Keep up-to-date on pending and final rules.
- Take CDD to deeper levels and identify all account owners and beneficiaries.
- Conduct IDV and eIDV, watch list screening throughout the life cycle of transactions through all access points.

However, the savings to your organisation and protection of national security will speak for themselves in the long and short run.

Keep your hands out of the flames and review your risk and your requirements on a regular and scheduled basis. **!**

Global Data Company (GDC), Bozeman, MT, USA, & Melbourne, AU, info@globaldatacompany.com

	NO	PARTIALLY	YES
Organisation-wide Risk Assessment (R.A.) is used to apply resources, develop procedures and controls. The target customer community is a factor in creating the R.A.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CDD steps and tools are not only applied at client entry point but throughout the life cycles of customer relationships, AND are applied to new co-owners, beneficiaries, etc. everywhere they appear after account or services are opened.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Watch list selections for the various high-risk areas of the organisation are chosen based on risks related to the business lines, geographic location of the business and the target customer community.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your company seeks input from your regulator about gaps you are aware of outside of an exam.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer activity and transactions are monitored against expected behavior and suspicious activity is flagged, taking into account the overall R.A. and target client community, geographic location etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your company has documented the staffing levels as being in alignment with the R.A. If not in alignment; documentation addresses a compelling reason as to why not.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Mobile money



Balancing
financial integrity
with business
expediency

Mobile money transfer (MMT) services have in recent years arguably been the single most effective contributor to global financial inclusion initiatives, and particularly in developing countries, have facilitated access to cheap and reliable financial services to an ever increasing unbanked population segment.

Recent innovations in mobile transfer services in countries, such as Kenya, have heralded unprecedented success in financial inclusion initiatives. In Kenya the M-Pesa service, which was pioneered by Safaricom Limited jointly with Vodafone UK in 2007, has received widespread international acclaim as the top ranking money transfer service globally. In recent years, innovations by Safaricom Limited have helped M-Pesa in Kenya grow from a simple money transfer service to a major payment service with millions of transactions worth billions of dollars annually. The services available under M-Pesa include retail purchases, Airtime Top Ups (Minutes), ATM withdrawals, international money transfers, medical and other charitable fundraising payments, bulk payment services through partnership with banks, insurance companies, micro finance, savings and credit societies, schools and other corporate organizations. These services facilitate the payment of regular and utility bills, banking transactions — including the transfer and withdrawal of funds from bank accounts, payroll and salary disbursements, loan disbursements and repayments, payments for goods, and school fees payments.

However, with the prevalence of mobile phones and the wide acceptance of MMTs as an alternative tool for financial inclusion in developing countries, MMTs and other financial institutions offering mobile banking services are fast becoming a soft target for mobile banking fraudsters, with those institutions lacking fully automated fraud prevention and transaction monitoring systems and controls being the most affected.

In this regard, the mobile money transfer service has rapidly become one of the preferred conduits for the perpetration of

fraud, largely due to the ease of delivery and the fact that it is a cashless service without face-to-face transactions, hence frontline, know your customer checks may not be possible on an on-going basis.

The escalation of mobile fraud has given rise to an increasing need to implement comprehensive AML programs in the mobile transfer and electronic payments sectors that are in line with the FATF recommendations. There also is a need to promote the sharing of information on AML best practises including suspicious transactions reporting, for the prevention of money laundering related fraud and financing of terrorism.

This need was underscored by the FATF Guidance Paper of June 2011 on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion whose primary objective was aimed at *interalia*, supporting efforts among competent authorities, across sectors and across jurisdictions that promote the complementarity of AML/CFT and financial inclusion. The guidance paper also supports the development of a common understanding of the FATF standards that are relevant when promoting financial inclusion and explicitly an understanding of the flexibility they offer with particular reference to the FATF risk-based approach.¹

The guidance paper specifically makes mention of mobile money as being among the “new financial products and services... created in the past few years which may contribute to expanding access to new markets and clients”² and advocates for appropriate controls in line with the overall objective of the paper.

Mobile money vulnerabilities to money laundering and terrorism financing

Mobile money has various risks which make it vulnerable to money laundering and terrorist financing.³

- *Delivery/Systemic Risk:* Its speed, portability and security make MMT a preferred service in developing countries and has led to the emergence of various mobile money frauds and scams

- *Geographic Risk:* Countries with deficiencies in AML controls, corruption, sanctions, and terrorist backgrounds will be more vulnerable to having their financial systems used for money laundering and terrorist financing activities
- *Product Risk:* There is the risk of unregistered users, minimal or no transaction limits, unregulated international money transfers and partnerships with third parties with inadequate or no AML programs
- *Customer Risk:* Countries with largely unbanked and/or illiterate rural populations and no identification regimes, or where there is an absence of easily identifiable residential and utility account information, will experience difficulties in the implementation of effective KYC and customer due diligence and, in particular, ensuring the quality of KYC information collected due to the lack of proper documentation and identification processes, and inability to store and retrieve customer information
- *Agent Risk:* MMTs with a large agent network, particularly in the rural areas, suffer challenges in implementing effective AML programs due to poorly trained agents leading to KYC compliance violations, inability to monitor high volume/high value transactions, lack of infrastructure and difficulties in carrying out regular due diligence and compliance monitoring on a large network
- *Training:* Difficulties in engendering a culture of AML awareness and suspicious activity reporting among the staff, agents and customers of MMT institutions
- *Resources:* The scale of mobile money in terms of customers, agents and transactions makes AML operations extremely resource intensive and many MMTs may not be in a position to afford the investment involved.

Common money laundering typologies in mobile money

The following are common typologies specific to mobile money transfers.⁴

¹ FATF Guidance PAPER of June 2011 on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion pg 9 objectives

² Ditto pg 16

³ Also see World Bank study on “Protecting Mobile Money against Financial Crimes, Global Policy Challenges and Solutions” <http://issuu.com/world.bank.publications/docs/9780821386699/1?zoomed=&zo>

⁴ ICA International Certificated Anti-money Laundering Awareness Training (UK) — Mobile Financial Services Module

1. Unregistered international money transfer services offered by informal money transfer agents
2. Suspicious agent activity outside the norm, which includes frequent deposits, multiple registrations, remote withdrawals, direct deposits etc.
3. Customers/agents registering multiple lines and/or carrying out multiple high value/high volume transactions to circumvent transaction thresholds
4. Hoaxes and scams/schemes to defraud unsuspecting customers
5. Bribery and corruption payments
6. Facilitation of payments for illegal activities/ predicate offences—cashless facility, multiple transfers/deposits
7. Kidnapping and extortion with ransom payments demanded through the money transmitter.

Financial integrity in mobile money: Implementation of an effective AML program

An effective AML program in line with FATF standards will entail putting in place the following measures:⁵

- Comprehensive AML policy and procedures encompassing training programs, continuous agent and staff awareness campaigns on KYC compliance and suspicious activity reporting
- Customer acceptance and identity verification at registration and thereafter for every transaction (KYC) for both individual and corporate customers
- Adoption of risk-based tiered KYC, for example no residential details or identification copy requirement on accounts with low level transactions
- Implementation of technology to capture KYC copies on higher risk accounts such as scanners or camera phones

- Customer profiling to categorize them depending on risk and business needs, for expanded migration to bill payment accounts for customers with high volume transactions to facilitate enhanced CDD
- Establishment of reasonable transaction limits depending on average business levels with systemic controls to prevent excesses
- Mandatory registration of all subscribers and restrictions on unregistered users
- Higher controls on IMT transactions and business usage
- Continuous AML awareness programs for agents, staff and customers including sensitization on various frauds and safeguard measures
- Automated suspicious transaction monitoring and watch list screening
- Suspicious activity reporting for customers, staff and agents
- Proactive risk assessments to protect M-Pesa and related services from being used for money laundering and terrorism financing
- Risk-based agent compliance monitoring programs focused on agents with high registrations or those in high-risk locations
- Agent penalty programs for non-compliance including warnings, fines, suspension of operation and claw back of commissions
- Appropriate deterrent action against fraudsters, including blocking/suspension of accounts with poor or duplicated KYC or accounts/lines that appear linked or have been used for fraud
- Profiling, arrest and prosecution of suspects involved in mobile fraud
- Recordkeeping and an audit trail for all transactions preferably using archiving systems which can electronically store customer KYC, agent due diligence and staff AML training records

- Regular engagement and proactive representations with regulatory agencies and business partners to benchmark on emergent trends and best AML practices and AML related fraud prevention measures.

Way forward

Mobile money is in a constant state of innovation and with the entry by non-MNOs—handset manufacturers/ nontelcos/banks/ and independent companies—into the arena and the provision of independent solutions such as mobile phone based MMT applications, there will be a need for increased regulation and greater cooperation between players. In this regard the benefits of technical interoperability between service providers will be worth exploring.

The contribution of MMTs toward the provision of access to financial services for the unbanked majority in developing countries, therefore, cannot be gainsaid. However, such innovation must go hand in hand with appropriate controls, and there is a clear need to balance controls with business expediency and the need for financial inclusion. Product risk assessment must be incorporated in every AML program in order to ensure all risks are identified and adequately mitigated with appropriate controls. **TA**

Mercy W Buku, LLB Hons (Nbi) CAMS, ACIB (UK), senior manager, Money Laundering Reporting Office, Safaricom Limited, Nairobi, Kenya, mbuku@safaricom.co.ke



⁵ Safaricom AML Policy and Procedures Rev 2012



ANALYTICS

Catch money launderers in the act.

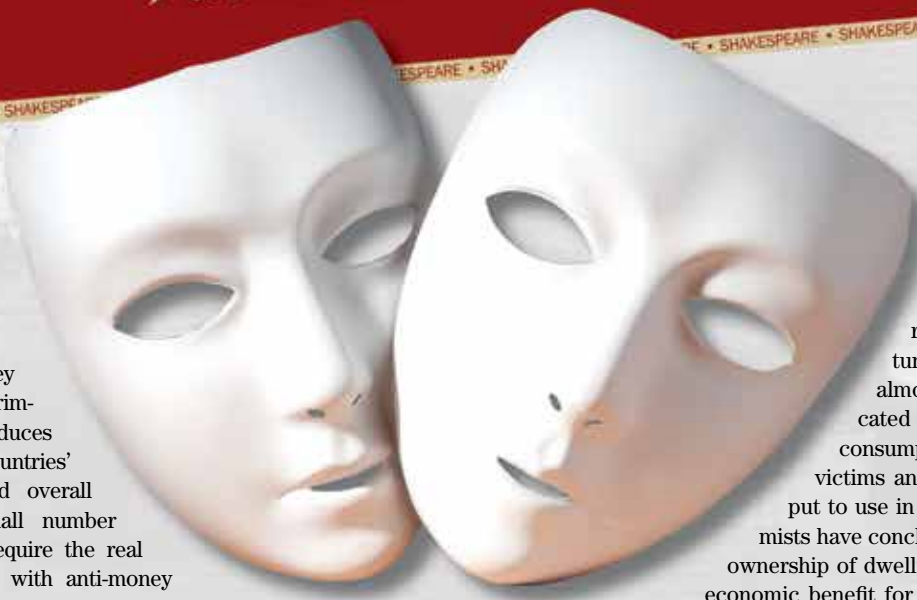
SAS® Anti-Money Laundering delivers dynamic risk assessment that classifies relationships as low, medium or high risk, so you investigate only meaningful alerts. Decide with confidence.



sas.com/alert
for a free white paper



All the world is real estate



In recent years, the use of the real estate sector for money laundering has increased significantly. Real estate money laundering supports criminal activities, and produces negative impacts on countries' real estate markets and overall economies. Only a small number of countries presently require the real estate sector to comply with anti-money laundering laws, and best practices for both preventing and identifying money laundering through the real estate sector have been slow in coming. This is surprising, given studies on the subject by both international and national anti-money laundering organizations, the large number of money laundering real estate related suspicious transactions filed, legal cases involving real estate, and media attention. There are a number of reasons for this.

The real estate business differs from country-to-country. Specifically, the ways in which real estate transactions are conducted worldwide differ significantly. Business practices differ. Regulations at the national and local level differ. Different cultural habits and values also play a role in real estate transactions. The size of the market also differs. Finally, technology has made real estate markets global through the use of the Internet. All these factors make it difficult to adopt uniform best practices. AML/CFT regulation of the real estate profession, much like other designated non-financial businesses and professions, has taken a back seat to the more central focus of financial intelligence units in banks and a few other entities like money services businesses. Another reason is that real estate professionals and lawyers

in many countries are fighting implementation of regulations, claiming the regulations are not necessary and would be unreasonably burdensome.

The large number of real estate transactions and perceived difficulty in identifying suspicious characteristics in real estate transactions may create the biggest obstacle. The answer to this obstacle is a risk-based approach. What would persuade countries to do more? Do we need to share more information about money laundering in the real estate sector, including the negative impacts, suspicious characteristics and AML/CFT best practices? Real progress is being made in a small number of countries which are providing information that can help in developing a risk-based approach.

Impacts of money laundering through real estate on markets and the overall economy

Money launderers often invest their proceeds of crime into real estate or other sterile assets such as high-value luxury items. A study in Australia of money laundering in real estate revealed a significant impact on Australia's econ-

omy. The Australians calculated that \$4.5 billion is laundered in the country and 23 percent of this is invested in real estate. Unfortunately, this amount, almost \$1 billion, is reallocated from other sectors to consumption of dollars from victims and drug users and not put to use in the economy. Economists have concluded that this kind of ownership of dwellings yields the lowest economic benefit for each dollar invested. This is supported by the economic multiplier effect of this reallocation in terms of changes to economic output, income demands and employment. The study estimated that when \$1 million is reallocated to real estate, there is an average net loss to the economy of \$1.43 million in output, \$576,000 in income and 20 jobs. By investing in real estate, money launderers also cause significant inflation in the real estate sector.

Africa, more than other parts of the world, may be experiencing greater increase in the use of real estate as a money laundering technique. During a recent assignment to Kenya, I was able to hear firsthand how money laundering is adversely impacting Kenya's real estate sector.

In Kenya, Somali pirates are taking proceeds from hijackings and laundering them in the real-estate markets of Nairobi and Mombasa. Because war-torn Somalia has been without a cohesive government for over a decade, conditions are poor and the country offers few opportunities for these criminals to launder money. Somalia investors have created an artificially inflated market in real estate in Nairobi, where buildings are going up everywhere

and house prices and rents have doubled. In suburbs in Nairobi, a four-bedroom home which sold for \$200,000 five years ago sells for \$500,000 today. Somalians now own estates that Kenya's middle class used to occupy. The area of Nairobi where most of the money laundering takes place is called Little Mogadishu, named for Somalia's capital city. Implementation of Kenya's anti-money laundering law has been slow. It has been only recently that the government has taken steps to make the financial intelligence unit operational. Like most countries with recent enactment of money laundering laws, real estate money laundering takes a back seat to money laundering in the banking sector. Perhaps regulating the real estate sector for money laundering should become a priority in Kenya.

Approaches to detecting and deterring money laundering through real estate

In developing regulations to detect and deter money laundering, countries should adopt regulations which fit the real estate market and existing regulatory framework in their country. Realtors are in the best position to utilize best practices for detecting and deterring money laundering because they are more knowledgeable of the buyers and sellers. Given the number of real estate transactions, it is essential that a risk-based approach be adopted that limits the amount of information required and focuses on the specific suspicious characteristics of money laundering through real estate.

Providing useful information of selected suspicious characteristics is a first step. Other African countries have recognized this need. In 2009, a group of West African countries belonging to the Inter-Governmental Action Group Against Money Laundering in West Africa participated in a comprehensive study of money laundering through real estate. The study "Typologies of Money Laundering through the Real Estate Sector" focused on the operations of real estate agencies and agents and included interviews with financial intelligence unit staff, real estate professionals and police. Among the most significant results was a list of 26 characteristics of transactions that could be indicative of money laundering.

In South Africa, both media and court reports describe the role of criminals in carrying out fraud schemes and of drug traffickers buying up or developing property.

The South African approach uses information from both government agencies and realtors. The Financial Intelligence Centre Act required real estate agents to conduct due diligence, maintain records and file reports when appropriate. Specifically, real estate agents must maintain the following information for five years:

- The identity of the client, client's agent, and client's client,
- The manner in which the identity was established
- The nature of the business relationship or transaction
- The parties to the business transaction and the amount involved
- All accounts involved
- The name of the person who obtained the information
- Copies of documents obtained by the institution.

South Africa's Estate Agency Affairs Board (EAAB) has been working with agents on compliance and raising awareness. Most important, the EAAB reassures agents of the confidentiality of filing suspicious transaction reports.

Providing useful information of selected suspicious characteristics is a first step

Efforts to develop a risk-based approach for both the real estate industry and government regulators are frustrated by both the large number of transactions and the number of suspicious characteristics. Researchers in the Netherlands have completed a study, the results of which have provided some assistance in this problem area. In the 2011

book, *Money Laundering through the Real Estate Sector*. Authors Brigitte Unger and Joras Ferwerda identify a total of 25 characteristics that render a property conspicuous (suspicious) and possibly being used for money laundering. One of the goals of the project was to differentiate conspicuous real estate transactions from all the ordinary ones. The study found the more conspicuous these properties are, the more likely there is to be money laundering involved. Characteristics that weigh heavier include (1) ownership by foreigners, (2) newly established companies and (3) properties with unusual price fluctuations. The more characteristics, the greater the susceptibility. The study was a collaboration between economists and criminologists who examined real estate transactions in two cities: Utrecht and Maastricht, Netherlands. For those countries which desire to trace money laundering patterns in selected cities, this model can be replicated in other countries.

In the development of a risk-based approach to money laundering through real estate, countries must study the roles of government regulators, real estate agents and other parties to the transactions. They must determine if agencies other than financial intelligence units such as registration agencies and real estate boards have the regulatory authority to perform some of the AML/CFT functions. They must determine what typologies of money laundering through real estate exist within the country. Finally, they must determine what regulations should be placed on the real estate industry that is both effective and the least burdensome.

Conclusion

Negative impacts from money laundering through real estate include support of crime, inflation in the real estate market and reduced activity in the overall economy. There is sufficient information available for countries to develop a risk-based approach uniquely suited to their country to deter and detect money laundering. More countries should undertake studies to determine the kinds of money laundering techniques that are unique to their country, in order to develop best practices for deterring and detecting money laundering in the real estate sector. **A**

James M. Wright, international banking consultant, Chartwell Compliance, Arlington, VA, USA, Jamesmwright01@aol.com

Reengineering compliance strategies as a counter-crisis measure



During the last two decades, the global communities' efforts in the fight against international crime organizations have been exponentially increased as far as property, capital seizure and control are concerned. Unfortunately these efforts have not had the desired effect when it comes to the movement of sources with illegal intentions and financing of criminal activities.

How can it be explained that even though the framework seems to be well structured and the governmental and law enforcement agencies are taking action as a communal force, the amount of capital flowing to the markets has not decreased and international crime organizations continue to drive economies to the point of breakdown by using crime proceeds and unfairly obtained money? The answer is clear — the structural problem that the compliance function has is hidden in the way in which it interacts with the target community and the perceptions that the community has of the regulator and its rules.

Marketing strategy and human behavior

The step forward is to involve a marketing strategy for human behavior modification as far as the compliance function is concerned. Regulators and agents are viewed as a barrier for growth and seen to set limits on the theory of accomplishment.

In this scenario, the business operation sees the compliance regulations as a major obstacle to performing their other functions on a daily basis. The tasks added to some workers and departments are seen as excessive, which creates a natural rejection of the compliance team and its work and goals.

The economic world crisis requires the opening of new markets and the establishment of improved procedures to gain resources without falling into the mistake of accepting crime proceeds that will deteriorate the global financial system and its ability to reflect accurate information about a country or business.

There are two factors that might come into consideration when creating a compliance department or when modifying an existing one. The first is that the economy does not answer to any other paradigms but its own. The second factor is that poor marketing strategies for compliance and sanctions departments represent a major comparative disadvantage.

The structural problem that the compliance function has is hidden in the way in which it interacts with the target community

The first issue is reflected in how law, psychology, marketing and policy development are limited by economic needs while the economy is not bound by the values and structures set by the other sciences or disciplines. This situation has left an economic market that only answers to itself and does not recognize social needs or policies. We have forgotten that economy is no more than a branch of praxeology, which analyzes decision making when facing a situation of shortage of resources.

The second factor of the compliance function having a poor or non-existent marketing strategy when developing policies starts with the name applied to the function and its approach to the people implementing its policies on a daily basis. It would be much more accurate and appealing to rename the function of compliance with a more meaningful label, such as "integrity" or "counter-crime department." This could help change people's behavior as they would be more willing to act to stop

criminality than to comply with a particular matter. Humans, especially in moments of crisis, tend to join causes that they consider superior, or which provide them with the feeling of belonging, while rejecting measures that impose more work or add tasks with a non-retributive structure.

In this case, after scanning the framework for compliance, we are approaching the problem from the wrong way. Instead of giving our departments a better appearance to improve perception, we continue improving the rule itself without a change of perception.

As marketing expert Rory Sutherland explained, there is no point in improving the food in a restaurant when the floor is dirty and disgusting smells are present. The food might be of the highest quality, but the perception will not change by improving the food even further, so the approach to the problem must change in order to have effect.¹

For policy makers, compliance officers and sanctions departments, reframing their function might have a greater impact in terms of efficiency than focusing on the technical solution for the problem itself. Knowing that it is already well regulated (and must continue evolving); this regulation is being poorly applied due to cultural barriers and a lack of communication with the final user.

A change in path

Following this line of thinking, AML specialists need to change from an aggressive imposed path to one in which the team members performing the task believe they are making a difference by taking action against the crime. In the end, every human being has a desire to feel his or her existence makes a difference and even better that he/she is a superhero in the fight against criminality. According to Sutherland, "If your perception is much worse than your reality; why on earth are you trying to change the reality."

Through small changes, the renewal of perspective about the role of sanctions/compliance and CDD becomes achievable. Thus, transforming the environment of

¹ http://www.ted.com/talks/rory_sutherland_perspective_is_everything.html

punishment and fear to a more enjoyable sense of importance of the task. In this new view of the compliance function, the present efforts of our regulations mix and interact with local values to produce efficiency.

Samuel P. Huntington understood and uncovered the importance of cultural and behavioral measures and their economic and politic importance by explaining the reconfiguration of the world order in his book *Crash of Civilizations*, stating that is not possible for a civilization to perform duties when they are against their beliefs or even more, when they do not rely on a set of values that are intrinsic to each culture, estate or country.²

In addition, compliance departments have failed to involve other departments in the risk analysis task by not recognizing their pivotal relation to the compliance matter and by disregarding the importance of other disciplines' knowledge into the complexity of the fight against criminal structures. We need to be part of the creative source of ideas in order to be important as

Compliance departments
have failed to involve
other departments in the
risk analysis task

product developers and tasks creators in order to make them user friendly and to create movements by inspiring the people performing the integrity function.

In conclusion, the challenge for this new era is simple but drastic:

- Compliance needs to involve creativity in the task development and policy creation/ implementation;

- Regulators and trainers must turn their actions to improve perception in the same way they are generating technical approaches to factual problems;
- Directors and managers need to apply behavior analysis and values scales to policy developments in order to make them user friendly and for the policies to be seen as a cause or campaign people can "be a part of" rather than an inconvenient and worthless task.

The fight against criminality requires all human capabilities and people committed to problem solving, not because they have to but because they are willing to and aware of their role in this universal fight. **▲**

Jaime Prieto, CAMS, compliance officer, Grand Duchy of Luxembourg, Luxembourg, prietoj@gmail.com

The opinions expressed in this article are those of the author alone, and not of any of the organizations that he represents.

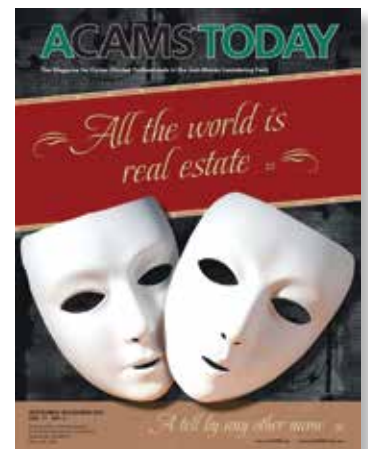
² <http://www.foreignaffairs.com/articles/48950/samuel-p-huntington/the-clash-of-civilizations>

Reading someone else's copy of

ACAMS[®] TODAY?

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

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



Association of Certified
Anti-Money Laundering
Specialists[®]

ACAMS[®]

For more information and to join contact us by:

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



BUILT FOR YOU.

A NEW INVESTIGATIVE PLATFORM:
CLEAR® FOR ENHANCED DUE DILIGENCE

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

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



Revving the innovation engine: Software as a service for AML and compliance

Following much criticism from federal examiners in 2010–2011, financial institutions have had to develop more effective Bank Secrecy Act and anti-money laundering (AML) compliance programs to address heightened regulation and enforcement. Meeting this challenge involves implementing business process improvements, recruiting additional staff and adopting enterprise-wide technology solutions for managing risk in a dynamic environment. Analysts agree that despite tight budgets and deferred capital investment, financial institutions have a need to update their technology. Celent predicts global spending on AML software will grow by 10.4 percent annually and reach \$5.8 billion by 2013. One of the factors contributing to this growth are AML vendors' delivery innovations.

SaaS — A leap forward

A closer look at recent trends in software delivery points to web-based, outsourced products and services that remove the responsibility for installation, maintenance and upgrades from over-burdened information technology (IT) staff. Organizations looking to reduce their IT capital expenditure and install software applications more quickly and efficiently are moving to Software as a Service (SaaS).

In a SaaS model, the application or service is deployed from a centralized data center over an Internet protocol (IP) network. The software and/or services, which are owned, delivered and managed by the provider, offer companies a flexible, cost-effective alternative to running software in-house. Enterprise markets are now embracing SaaS since the model has matured and initial concerns with security, response time and service

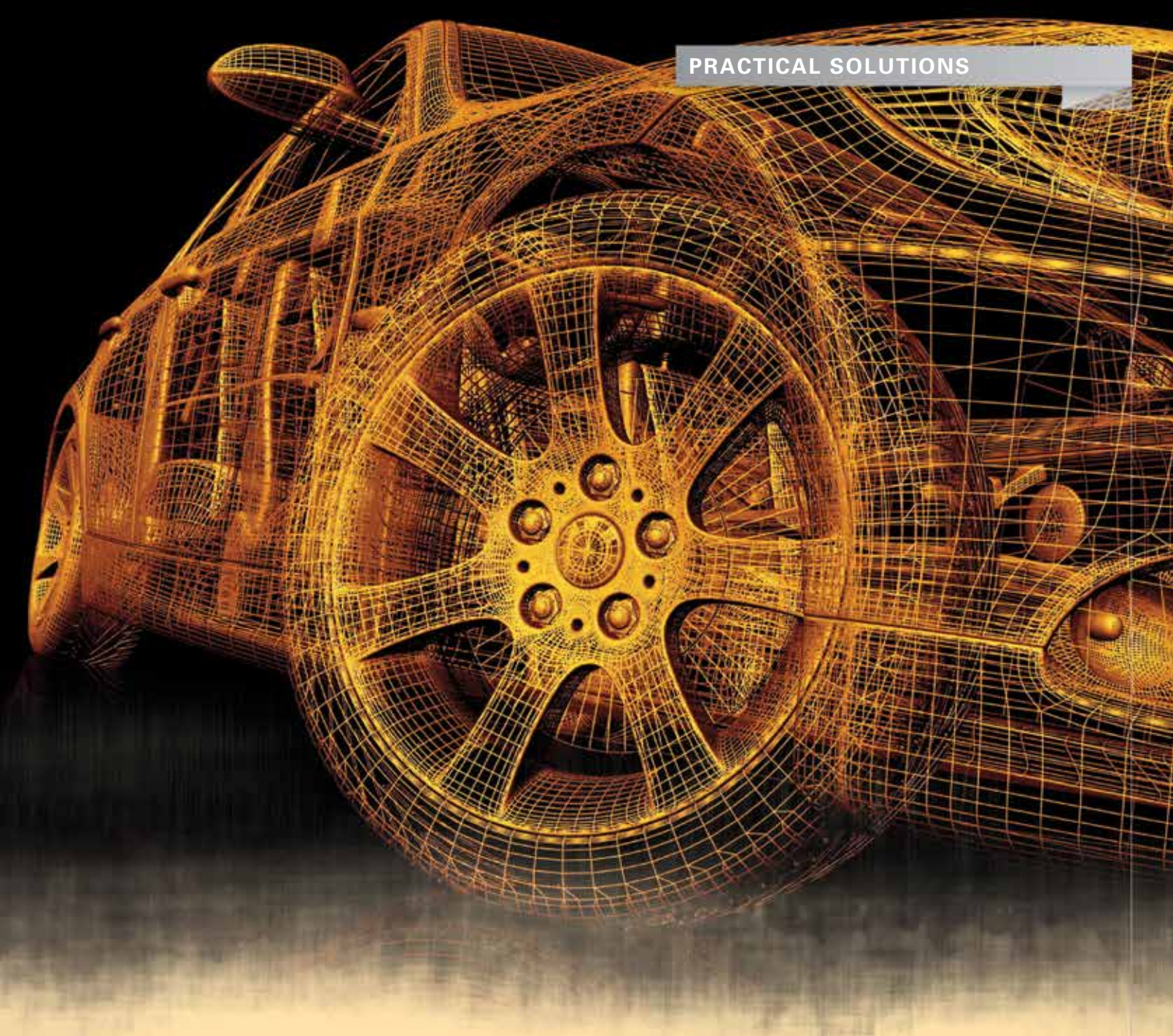
availability have diminished. Although the market is still in its early high-growth phase, SaaS models are becoming part of the mainstream as they move beyond customer relationship management (CRM), human resources and procurement into business intelligence, eCommerce and IT infrastructure. A 2011 Gartner survey of 525 organizations and 12 vertical industries in nine countries indicated nearly 70 percent of organizations have used SaaS for less than three years. While previous surveys reported the use of SaaS as an extension to existing on-premises applications, in 2011 the leading uses were either replacements for on-premises applications or new SaaS solutions. Current trends forecast the expansion of the SaaS model to "everything as a service." But the question remains: Are financial institutions ready to buck tradition and consider a SaaS alternative for enterprise-wide AML and compliance?

The Internet has fueled an outbreak of financial crime. Cybercrime and identity theft cost the global economy approximately \$114 billion in 2011. As organizations with budget and resource constraints struggle to keep pace amid the barrage of money laundering, fraud and other criminal activity, robust and affordable systems with surveillance functionality are needed to mitigate increased risk. Automating compliance requirements in a dynamic regulatory environment continues to be problematic. The solution lies in technology that is scalable, cost effective and offers a shorter time to production. This has prompted an often lively debate within the financial community over SaaS versus the traditional and still more prevalent on-site platforms.

Eliminating the roadblocks

Business and compliance users are often frustrated by the long deployment cycles, skyrocketing costs, demanding upgrade processes and complicated IT infrastructure of on-premises solutions. Analyst surveys indicate that business users drive SaaS decisions while their IT counterparts remain skeptical. Key concerns include data and systems integration, security and governance. SaaS providers have made significant efforts to address these issues particularly as they relate to data privacy, protection and security. Industry standard audit controls and SAS 70/SSAE 16 certifications have increased confidence in SaaS for more mission-critical applications including those supporting AML and compliance functions.

Building an enterprise-wide platform is a daunting, costly, and labor-intensive task. While most institutions prefer to have third-party applications installed in-house, changes in the regulatory environment are happening so fast that business and IT leaders must collaborate in real time. SaaS relieves IT staff of many tasks throughout the software lifecycle and creates greater opportunities to strategize with business and compliance colleagues on short- and long-term requirements. Grappling with poor data quality and inconsistent information from disparate systems could put an institution at risk. This should motivate decision-makers to pursue the most cost-efficient, state-of-the-art, integrated platforms from which to monitor enterprise risk. Those seeking innovative strategies to streamline processes and control costs must give serious consideration to SaaS as a viable option for AML and compliance operations.



While the SaaS adoption rate for AML and compliance is growing, it is not without challenges. There is still hesitation about sending customer data off-site. Vendors have responded by strengthening data leakage controls and implementing other security measures in order to satisfy the strict requirements imposed by risk management and security oversight groups. The argument for on-site solutions is weakening as hosted benefits are significant enough to persuade the skeptics.

SaaS for AML and compliance adds value from a strategic as well as a practical standpoint. The degree of automation and scalability can provide an enormous advantage for managing risk across the enterprise. Lower cost of ownership

and shorter time to production enables IT, business and compliance groups to become more agile partners in managing the intersection of compliance and technology. The mobility of applications delivered via the Internet can greatly improve efficiency and resource utilization especially for global operations. An effective SaaS platform has the potential to be a game changer in protecting the reputation and assets of an institution.

Getting on the SaaS bandwagon

A KPMG survey reports that unfavorable economic conditions and regulatory reform are casting new light on traditional business models. Respondents in the banking sector identified regulatory and legislative pressures

as the most significant barrier to growth in the near term. Industry experts seem to agree that few, if any, applications are too big or too critical for SaaS. They encourage organizations to be forward thinking and adopt innovative strategies that include SaaS. No doubt, SaaS is here to stay. As the cost of combatting financial crime continues to climb and penalties for non-compliance increase, institutions focused on the core value of enterprise-wide risk management will include Software as a Service for AML and compliance in their strategic plans. **A**

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

A tell by any other name

—What a poker player can teach you about recognizing suspicious activity



Gambling is inherently a risky business and one where the odds of success run from slim to practically none. Yet the game of poker injects both a skill element born of study and experience and the element of psychology that can significantly mitigate the risks for a skilled and dedicated player. While there is still the element of randomness that can defeat even the most highly rated player, playing against humans provides what a roulette wheel and rolled dice cannot. That is a clue to what your opponent is doing and planning — which in poker parlance is called a “tell.”

There is a similarity in poker tells and money laundering red flags in that some are very easy to spot and others take a significant amount of skill, intuition and perseverance to recognize. Whether you are a seasoned anti-money laundering (AML) professional

or a rank beginner, a primer on recognizing money laundering red flags is a useful tool. Certain aspects of a poker game and the actions of poker players have remarkable similarities to the classic three stages of money laundering.

For example, the stakes of the game and preference of opponents equates to placement, as it involves selecting the best means of entering money into the “game.” The ways bets are placed are physical clues depending on holding a winning, marginal or bluffing hand equates to layering. This is how your opponent is manipulating the way the money is either placed at risk for greater profit or shielded from those who seek it. The final bet to lure you into a losing call or fold equates to integration. When the poker player leaves the tables with his or her winnings, the money has been removed from the “game.”

Collecting enough useful knowledge about a poker player or a money launderer is not always an easy task. The movies may depict a poker tell as a nervous cough, sitting forward or blinking the eyes rapidly. If only it were that easy. Professional players collect data over a period of time and are constantly noting aspects of an opponent’s personality, tendencies and style of play. In addition, they are constantly seeking updated information as their opponents will often change their style to throw others off. However, there are still patterns that can be discerned and profiles that can be created if one is observant and dedicated enough to spot them. So it is with spotting the indications of money laundering. Knowing what tells or red flags to look for can go a long way in the risk mitigation function of your AML efforts. What follows is a condensed view of sample red flags at each of the three

stages of money laundering. These samples come primarily from the banking and financial account industries, though there are some useful insights for money services businesses as well.

The following examples are meant to help compliance officers identify certain types of transactional activity during review of their everyday reports. These are only a few examples of many and this will hopefully help to develop a reporting structure to make a more efficient and well documented AML program. These examples are simple and brief, but as we all know, good launderers often have very complex and intricate laundering schemes.

There are a number of sources for discovering and detailing the various red flags. Many of them are the same for most of the examples that follow. Instead of listing them repeatedly for each scenario, here is a list of excellent sources of data that will enable you to spot those trends and patterns that lead you to catching a money launderer.

Red flag source materials:

- CIP/CDD reports
- Web searches on customers and signers
- Bank documentation
- Cash reports
- ACH reports
- Wire reports
- Internal transfer reports
- Monetary instrument purchases
- Reports on associated accounts
- Velocity reports
- Information from tellers and other front-line staff

Placement

When you first join a poker game you want to be knowledgeable about your opponents or be able to size them up pretty quickly. This gives you an advantage from the start. The same is true of spotting money launderers.



Classically, the first and most vulnerable stage of laundering money is placement. Your opponents are working hard to put their illegal proceeds into the financial system/game without attracting attention. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. Therefore, the initial place to focus on finding flags for AML professionals is cash transactions.

Placement red flags:

- Exact dollar amounts
- Large amounts of cash-ins that are not in line with a type of business.
- Cash-intensive businesses that split their deposits to avoid reporting requirements
- For high cash volume businesses, none of the cash-ins are over \$10,000.00
- Cash-ins in some cases are performed on the same business day, however, different branches are used

Information derived from the backroom review:

- Exact amount cash-in
- Any linkage between customers noted in CIP/CDD information
- Look for where the funds go, review the destination of funds

When sizing a potential money launderer or a poker opponent there is nothing like first-hand information. What your frontline staff can tell you is invaluable. Make sure they are well trained to pick up on certain behaviors.

For example:

- Exact amount cash-ins

- Any comments the customer makes concerning the transactions or their business
- Any mention of the reporting thresholds when deposits made

Supporting documentation (your little black book on your opponents):

- Document any notes from the frontline on comments the customer may have made
- Document the source and destination of funds
- Document all web searches for information on the customer and customer's business

Here's an example of a placement scenario relating to real estate. Smart 1 is a real estate business. In reviewing cash reports it is noticed there are numerous high dollar cash-ins, the cash-ins are exact amounts and are all under the reporting threshold. The cash-ins are made at different branches on the same business day in some cases.

In order to spot this type of placement, perform red flag reviews of your reports. Sort the reports by branch and date to find customers performing cash-ins around the same time every day. Also, look for customer associations.



Your backroom staff should take a close look at customers via CIP reports and business signers. Create transparency with the customer to know who benefits from the funds. This aspect is becoming more and more important as the regulations are requiring you to dig even deeper into the beneficial ownership of an account. In addition, look at the destination of the funds deposited. See if the deposits are transferred or put into a shared or associated business account.

Let us look at how this scenario plays out on a spreadsheet. In Table 1 below see how the exact dollar amounts of cash-in are structured over multiple days, as well as some deposits made on the same day at different branches. Note the business type and research to see why a real estate business may have large cash-ins. Remember to document any findings. If it is not documented it might as well have never happened.

Here is another placement scenario that should instantly alert you to deposit activity that is out of the ordinary. A customer that you know works for a construction company that makes large cash deposits containing many larger denomination bills, such as the

500 euro note or US\$100 bills. This customer will frequently deposit large sums of cash wrapped in currency straps stamped by other banks or currency wrapped in rubber bands that is disorganized and does not balance when counted. This kind of red flag is one of the easier ones to spot. It is like the “nervous cough” tell of a poker player with a great hand.

Note from the transactions in Table 2 below the exact amount of cash-in under the reporting threshold (\$10,000.00) on consecutive days. Remember to document any information from the teller as to how the cash is deposited, for example denominations strapped or unstrapped.

Sometimes you will come upon a poker game where it quickly becomes obvious that certain players are working together or have established a pattern that would indicate some sort of collaboration. This is the same as structuring through “smurfing.” An alert frontline staff will pick up on the consistency and frequency of some depositors. It can also be spotted by a review of cash-in reports.

In Table 3, Joe Smith is noticed purchasing several cashier’s checks for cash in amounts that would not be recorded. Note the cash-in for cashier’s check purchases under the \$3,000 amount as some people see the \$3,000 cash-in for cashier’s checks as a reporting threshold. Look at the payees on the checks

Table 1

Acct#	Acct Type	Name	TIN	Branch	Date	Description	Amount	Cash In	Cash Out	Business Type
111111111	DDA	Smart 1	545454545	1	7/31/2011	Deposit - Commercial	\$ 5,000.00	\$ 5,000.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/1/2011	Deposit - Commercial	\$ 4,500.00	\$ 4,500.00		Real Estate
111111111	DDA	Smart 1	545454545	2	8/1/2011	Deposit - Commercial	\$ 5,000.00	\$ 5,000.00		Real Estate
111111111	DDA	Smart 1	545454545	3	8/1/2011	Deposit - Commercial	\$ 4,000.00	\$ 4,000.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/2/2011	Deposit - Commercial	\$ 9,600.00	\$ 9,600.00		Real Estate
111111111	DDA	Smart 1	545454545	2	8/2/2011	Deposit - Commercial	\$ 7,000.00	\$ 7,000.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/3/2011	Deposit - Commercial	\$ 7,500.00	\$ 7,500.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/11/2011	Deposit - Commercial	\$ 3,000.00	\$ 3,000.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/12/2011	Deposit - Commercial	\$ 3,600.00	\$ 3,600.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/21/2011	Deposit - Commercial	\$ 8,500.00	\$ 8,500.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/22/2011	Deposit - Commercial	\$ 9,000.00	\$ 9,000.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/29/2011	Deposit - Commercial	\$ 6,000.00	\$ 6,000.00		Real Estate
111111111	DDA	Smart 1	545454545	2	8/29/2011	Deposit - Commercial	\$ 6,500.00	\$ 6,500.00		Real Estate
111111111	DDA	Smart 1	545454545	1	8/30/2011	Deposit - Commercial	\$ 4,500.00	\$ 4,500.00		Real Estate
111111111	DDA	Smart 1	545454545	2	8/30/2011	Deposit - Commercial	\$ 5,000.00	\$ 5,000.00		Real Estate

Table 2

Acct#	Acct Type	Name	TIN	Branch	Date	Time	Description	Amount	Cash In	Occupation
222222222	DDA	Denise Menace	121212121	1	8/1/2011	9:00 AM	DDA Deposit - Personal	6,000.00	6,000.00	Construction
222222222	DDA	Denise Menace	121212121	1	8/2/2011	10:15 AM	DDA Deposit - Personal	5,000.00	5,000.00	Construction
222222222	DDA	Denise Menace	121212121	1	8/4/2011	10:30 AM	DDA Deposit - Personal	5,500.00	5,500.00	Construction
222222222	DDA	Denise Menace	121212121	1	8/5/2011	10:00 AM	DDA Deposit - Personal	10,000.00	10,000.00	Construction

Table 3

Acct#	Acct Type	Name	TIN	Branch	Date	Description	Amount	Cash In	Cash Out	Business Type Code
123456789	DDA	Joe Smith	787878787	3	8/1/2011	Purchase Cashiers Check	2,500.00	2,500.00		Unknown
123456789	DDA	Joe Smith	787878787	8	8/11/2011	Purchase Cashiers Check	2,500.00	2,500.00		Unknown
123456789	DDA	Joe Smith	787878787	9	8/18/2011	Purchase Cashier’s Check	2,500.00	2,500.00		Unknown
123456789	DDA	Joe Smith	787878787	1	8/22/2011	Purchase Cashier’s Check	2,500.00	2,500.00		Unknown
123456789	DDA	Joe Smith	787878787	1	8/30/2011	Purchase Cashier’s Check	2,500.00	2,500.00		Unknown
123456789	DDA	Joe Smith	787878787	1	8/1/2011	Purchase Cashier’s Check	2,500.00	2,500.00		Unknown
123456789	DDA	Joe Smith	787878787	1	8/2/2011	Purchase Cashier’s Check	2,500.00	2,500.00		Unknown
123456789	DDA	Joe Smith	787878787	1	8/4/2011	Purchase Cashier’s Check	2,500.00	2,500.00		Unknown
123456789	DDA	Joe Smith	787878787	1	8/5/2011	Purchase Cashier’s Check	2,900.00	2,900.00		Unknown
123456789	DDA	Joe Smith	787878787	1	8/18/2011	Purchase Cashier’s Check	2,900.00	2,900.00		Unknown

Caught in the storm?

FATCA**FINRA 2090/2111****Customer Due Diligence****SAR Filing****Watch List Screening****CTR Reporting****Suspicious Activity Monitoring**

NICE Actimize has a deep understanding of the challenges financial institutions face as they seek to control costs associated with addressing heightened regulatory scrutiny, adapting to changing global compliance requirements, and managing the risk of introducing new products. Whether your focus is retail, commercial or investment banking, brokerage or insurance, NICE Actimize can provide integrated BSA / AML and financial crime solutions that ensure effective compliance and future-proof your business.

NICE Actimize enables financial institutions of all sizes to share and consolidate information across the organization, improve operational efficiency, and mitigate risk with industry-leading AML, fraud, and enterprise case and investigation management solutions. Whether challenged to satisfy updated regulations such as FATCA, CDD, and FINRA 2090 / 2111 rule changes; meet new SAR / CTR reporting requirements; or improve the effectiveness of BSA / AML programs, NICE Actimize has the solutions and expertise to help.



Platinum Affiliate Member

Contact us today to learn more about how we can help your organization: info@actimize.com**New York:**
212 643 4600**London:**
44 (0) 20 7255 1065**Hong Kong:**
852 2598 3838

and note if they are the same or different, to a business or to a person and what the relationship may be.

Layering

Layering is the midgame of the money laundering process. It is often the most complex and convoluted, therefore making it the hardest to trace. The shell game of moving funds around the financial system in a complex series of transactions to create confusion and complicate the paper trail makes finding the red flags that much more difficult. It is the same with trying to figure out a world-class poker player. Players at the top level know you are trying to find their tells, so they work hard to hide them. Common examples of layering include exchanging monetary instruments for larger or smaller amounts, wiring or transferring funds to and through numerous accounts in one or more financial institutions. The trick is knowing what to look for and anticipating the money launderer's next move based on previously created, well-researched profiles.

Layering Red Flags:

- Many transactions with exact dollar amounts, but not all the time
- Velocity of funds into and out of accounts
- Internal transfers between accounts
- High volume of wires and ACH transactions in and out

What to look for in the reports:

- Transactions with exact dollar amounts, any linkage between customers noted in CIP/CDD information
- Destination and source of funds



Important information from frontline staff:

- Transactions with exact dollar amounts
- Any comments the customer makes concerning the transactions or their business
- Any mention of the reporting thresholds when the deposits were made

What to have in your little black book:

- Document any notes from the frontline on comments the customer may have made
- Document the source and destination of funds
- Document who the funds go to or come from and any linkages found in the review
- Document all web searches for information on the customer and customer's business

The examples of layering could fill volumes so here's a common one:

The customer withdraws cash, in \$100 bills, in amounts under the reporting threshold, from accounts where funds derived from fraud schemes were deposited. Those funds are then wired to an offshore account where they are consolidated and used to buy goods.

By some standards that is a relatively simple trail. To latch onto the layering scheme one needs to be able to see the big picture and assemble a collection of transactions into a cohesive story. Often the first steps in this process show up in some of the reports that were mentioned earlier. For example:

- From review of backroom reports look for large exact dollar withdraws
- Look for source of funds for the withdrawal look for possible fraud red flags
- Train frontline staff to note denominations

Here's what the extraction of funds to start the layering process might look like. From the Table 4 below you can see exact amount of funds-in from PayPal also look for other money transfer vendors. Look at the velocity of funds in and funds out and source and destination of funds. Don't forget to document any findings.

Integration

A poker player wants to leave the table with a large stack of chips, especially those chips that used to belong to someone else. Often his opponents know they have been beaten, but are often not sure how. That in a way is the same goal as a money launderer. They want to integrate the money back into the world in legal funds even though they started the journey with a criminal origin. The integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the

Table 4

Acct#	Acct Type	Name	TIN	Branch	Date	Description	Amount	Cash In	Cash Out	Business Type
11111111		Smart1			7/31/2011	ACH In Pay Pal	\$5,000.00			Real Estate
11111111	DDA	Smart1	545454545	1	8/1/2011	Cash on us check	\$4,500.00	0	\$4,500.00	Real Estate
11111111		Smart1			8/1/2011	ACH in Western Union	\$5,000.00			Real Estate
11111111		Smart1			8/1/2011	ACH In Pay Pal	\$4,000.00			Real Estate
11111111	DDA	Smart1	545454545	1	8/2/2011	Cash on us check	\$9,600.00	0	\$9,600.00	Real Estate
11111111		Smart1			8/2/2011	ACH in Western Union	\$7,000.00			Real Estate
11111111	DDA	Smart1	545454545	1	8/3/2011	Cash on us check	\$7,500.00	0	\$7,500.00	Real Estate
11111111		Smart1			8/11/2011	ACH in Western Union	\$3,000.00			Real Estate
11111111	DDA	Smart1	545454545	1	8/12/2011	Cash on us check	\$3,600.00	0	\$ 3,600.00	Real Estate
11111111		Smart1			8/21/2011	ACH In Pay Pal	\$8,500.00			Real Estate
11111111	DDA	Smart1	545454545	1	8/22/2011	Cash on us check	\$9,000.00	0	\$ 9,000.00	Real Estate
11111111		Smart1			8/29/2011	ACH In Pay Pal	\$6,000.00			Real Estate
11111111	DDA	Smart1	545454545	1	8/30/2011	Cash on us check	\$6,500.00	0	\$ 6,500.00	Real Estate
11111111		Smart1			8/29/2011	ACH in Western Union	\$4,500.00			Real Estate
11111111	DDA	Smart1	545454545	1	8/30/2011	Cash on us check	\$5,000.00	0	\$ 5,000.00	Real Estate

source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts or other assets.

Integration red flags:

- Transactions with exact dollar amounts
- Look for large dollar purchases that are unexplainable
- Review large payments off to loans or credit cards

What to look for in the reports:

- Transactions with exact dollar amounts
- Any linkage between customers noted in CIP/CDD information
- Look for where the funds come from and go to, review destination and source of funds

Important information from frontline staff:

- Transactions with exact dollar amounts
- Any comments the customer makes concerning the transactions or their business
- Any mention of the reporting thresholds when performing transactions (not just cash)

What to have in your Little Black Book:

- Document any notes from the frontline on comments the customer may have made
- Document the source and destination of funds
- Document all web searches for information on the customer and customer's business

A typical integration scenario involves the purchase and resale of real estate. In it a customer makes frequent loan payments for

large exact amounts, you may notice a short time period in the loan disbursement and the payoff of the loan.

Some of the ways to spot this are:


- Look for large exact dollar payments from reviewing backroom reports
- Review type of business or customer's occupation
- Review loan documents to see purpose of loan
- Research related documents that can be helpful for further due diligence (financial statements, tax returns, etc.)
- Conduct web searches on business and / or customer to find more information on the customer
- Document source of funds for the payments and destination of funds for the loan disbursement look for possible red flags

From Table 5 below you can see exact amount of funds going to make loan payments either directly to the loan or from a checking account the funds went into. Be sure to adjust your thresholds and look periodically at all transactions-in and out to see if there are holes in the report that need to be fixed and thresholds need to be updated. Depending on your organization's risk appetite, you may need to assess the thresholds at least quarterly. Also, look at the velocity of funds in and funds out and source and destination of funds, document any findings.

Seeing the big picture

As stated previously, few poker players have simple tells. Identifying the tells and red flags of your opponents takes detailed, integrated study, and sometimes a little luck, to uncover. Money laundering schemes are difficult to

uncover especially in the later stages. It is through research and good documentation — the little black book — that you can eventually put pieces of the puzzle together as you go. Looking at all the stages together may help to see a possible case and work to help uncover crimes that may be occurring. Graphics often make it much easier to spot telltale trends as they can illuminate data that could get lost in endless spreadsheets, even with computerized programs to help pull data. For example using pivot tables to visualize transactional activity either through graphs or through flow charts may help to paint a picture not seen in normal reports. Visualizing where the funds go and how they go into and out of accounts is a great tool in investigating activity.

Whether you are planning on entering an international poker tournament or breaking a worldwide money laundering ring, looking for tells and red flags as part of a bigger picture and documenting them effectively is the best formula for success. Stay alert, stay focused and pay attention to details. That's the best bet for coming away with a winning hand. 

Robert Joe Sniat, CFE, CAMS, BSA/AML officer, Union First Market Bankshares, Richmond, VA, USA. The presentation that is the basis of this article can be found at www.ACAMSToday.org or by emailing robert.sniat@bankatunion.com

Ed Beemer APR, CAMS, principal, ComplianceComm®, a BSA/AML compliance communications firm in Arlington, VA, USA, efb@compliancecomm.com

Grant Brownrigg of Grantland.net created the artwork for the article.

Table 5

Acct#	Acct Type	Name	TIN	Branch	Date	Description	Amount	Cash In	Cash Out	Business Type
22222222	Loan	Smart1	545454545	1	7/31/2011	Loan	\$200,000.00			Unknown
11111111	DDA	Smart1	545454545	1	7/31/2011	Transfer from Loan	\$200,000.00			Unknown
11111111	DDA	Smart1	545454545	1	8/1/2011	Wire out Title Settlement	\$200,000.00			Unknown
22222222	Loan	Smart1	545454545	1	8/12/2011	Loan Payment	\$50,000.00			Unknown
22222222	Loan	Smart1	545454545	1	8/13/2011	Loan Payment	\$25,000.00			Unknown
22222222	Loan	Smart1	545454545	1	8/29/2011	Loan Payment	\$25,000.00			Unknown
22222222	Loan	Smart1	545454545	1	8/30/2011	Loan Payment	\$25,000.00			Unknown
11111111	DDA	Smart1	545454545	1	9/9/2011	Loan Payment	\$25,000.00			Unknown
11111111	DDA	Smart1	545454545	1	9/22/2011	Loan Payment	\$25,000.00			Unknown
11111111	DDA	Smart1	545454545	1	10/1/2011	Loan Payment	\$25,000.00			Unknown

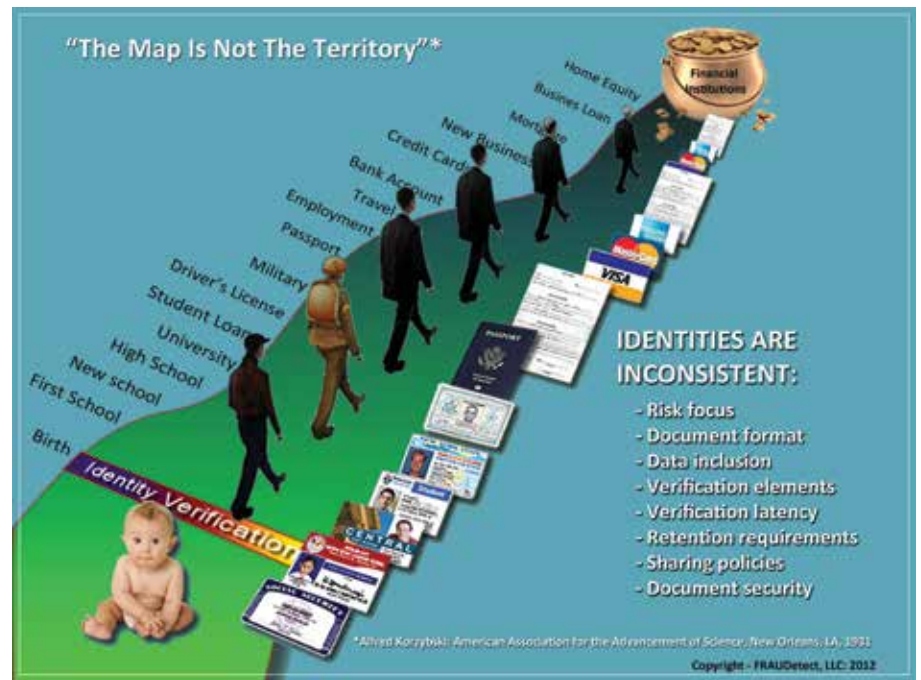
Changing the identity management paradigm

As anti-money laundering (AML) and financial crimes compliance professionals, we are focused on preventing money laundering, terrorism financing, fraud, waste and abuse. While conducting our work, we have to recognize the vulnerabilities in our current thinking about identity verification and authentication across the entire financial institution enterprise.

The problem we have is that:

- We begin enrollment, onboarding and other Customer Identification Program/ Know Your Customer (CIP/KYC) processes with different Personal Identity Information (PII) documents that are created for different purposes and have varying reliability (e.g., driving, taxes, employment, citizenship, education, military, etc.). These documents possess different PII elements, employ different formats and levels of security, vary in period of validity, retention and sharing policies.
- Once enrollment and verification are completed, we assume in our authentication processes that the validity of the identity and the associated risks remain static. We rarely relate the identity risk to identity use and the transactions that depend upon it.
- There is rarely, if ever, a feedback loop that revalidates and adjusts identity risk based upon identity use and transactional behavior.

Consideration should be given to implementing an Integrated Identity Management (IIM) process that incorporates the principles of a complete system in which: input and output are measured; security is layered and diversified throughout; the most modern combinations of technology are blended; identity use and related transactions are monitored, tracked and evaluated; and a



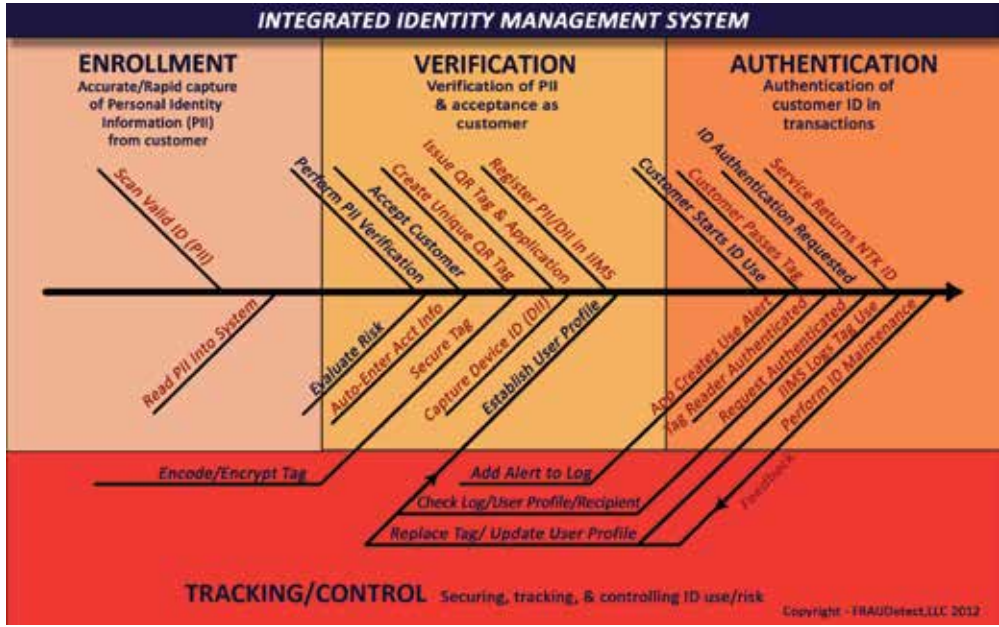
solid feedback method detects and warns of behavioral changes and risks. Such a process must incorporate cost efficiency as a principle goal and use reliable methods to reduce labor and increase both accuracy and reliability.

A new paradigm is possible that can:

- Scan PII data directly from a valid 2D bar code or identification card with a magnetic strip into a verification process. (*Eliminating keystroke errors*)
- Evaluate verification results and automatically enter approved PII into bank account opening forms. (*Eliminating keystroke errors, duplicate entry and reducing labor*)
- Capture device identity information (DII) from mobile phones and marry this with PII. (*Creating a new dimension of identification and tracking*)

- Issue a highly secure encoded/encrypted unique quick response (QR) tag to the individual for controlled identification. (*Maintaining true, verifiable identity on each transaction*)
- Track transfer of identity information, monitor transactions for risk and update identification profiles. (Monitoring and adjusting for risk in identity profile and use)

The approach uses scanning and auto entry systems to capture data from a valid identity card. While using conventional PII verification methods, the IIM expands from traditional methods by adding in DII as a component of the individual's dynamic identity. The DII provides not only the specific static information for the customer's wireless device, but it also is employed later in the authentication and transaction analysis processes to provide location and other dynamic information. A unique QR Code



computer and the devices will have communication features and speeds that will further drive growth in the mobile space. One of the important features of the smartphone is its ability to display high resolution images. This is not only a value for accurately reading QR codes, but it also permits display of individual identity photos in high quality. Combining accurate, high quality facial images with a series of knowledge-based questions, obtained from a highly secure process, can produce significant improvement in assuring true identity transactions.

Customer identification can no longer be treated as an independent event at the beginning of a continuing business relationship; and then assumed to remain valid indefinitely in today's dynamic world. In addition, identity verification and authentication of customers must be holistic. Systems must address enterprise-wide needs, including diverse business and services verticals across the financial institution.

(ID Tag) carries encoded and encrypted information about the individual's identity and is maintained on the wireless device by a high security application, or the tag can be printed on a card or used on a PC. The tag can be transmitted visually, by SMS, email or through the Internet. Since the actual identity information resides on a remote server, a series of logging, risk assessment, authentication and monitoring steps are included to ensure that risk for each transaction is assessed and feedback is provided for changes to the individual's profile.

The above fishbone chart depicts some of the functions of an IIM that will enhance AML customer risk controls and also protect against identity theft and fraud. New/added functions are in red.

As anti-money laundering and counter-terrorism financing remain key government objectives for the financial industry, the complexity of both criminal methods and regulatory compliance continues to increase. Laundering and other suspicious activities, like those associated with Summer Work Program/J1 visa risks, continue to provide serious challenges for customer identification and enhanced due diligence programs.

Consider the advantages of an Integrated Identity Management System for tracking potentially high risk customers for AML compliance. The system can be implemented for all or only certain groups of customers. For example, suppose we wanted

to track customers with ITINs and J1 visas. These individuals could be issued a unique tag that could reside on a cell phone, a bank identification or debit card. A printed label with the tag could be fixed to other identity documents required for use in bank transactions. By reading the tag at each transaction with the bank, the members of the group could be tracked by frequency of use, location of use (GPS), risk profile, profile (i.e., behavior) changes and transaction type.

The mobile payments industry is a driving force for the expanded use of wireless communications. At the beginning of 2012 there were 100 million smartphones in service in the U.S. and growth in this technology is expected to remain at 15 percent per year for the next five years. Within that time, the computational power in a handheld device will be equal to today's personal

The knowledge of PII must be maintained as it evolves; it must be protected with more than simple passwords and user authentication, and must be adaptable to the rapidly evolving needs of mobile commerce. The Integrated Identity Management System described herein is a paradigm shift from the past and into the future. It recognizes the vulnerabilities of today and the needs of tomorrow by employing the latest highly mobile and responsive technology embodied in smartphones, QR codes, advanced encoding and encryption, profile and behavior analysis, and other security measures. The benefits of the approach focus on both the institution and the individual. Finally, the methods described produce a true prevention process that can eliminate the threats of identity theft and fraud and their impacts on the banking industry. **A**

Bob Cofod, president and founder of FRAUDetect, LLC, Churchton, MD, USA, bob.cofod@bankdetect.com

Rob Goldfinger, CAMS, CFS, president, Lormel Goldfinger Global Group, LLC, Holly Spring, NC, USA, rgoldfinger@lormelgoldfinger.com





The need for improvement

With changing regulation, increasing market competition and consolidation — especially within the context of the current financial crises, banks and other financial institutions need to better manage risk, reduce cost and increase revenues.

Know Your Customer (KYC) is a niche business process and is often costly and inefficient. The real direct and indirect people costs are high and continue to increase. KYC is also a non-core competency requiring the

continuous retraining of a wide range of senior staff and reinvestments in non-revenue-generating policy, procedure and process definition. As an often inefficient and infrequently performed non-core activity, quality and morale can suffer, leading to audit issues such as incomplete or out-of-date files and AML customer events going unrecorded or non-investigated. Furthermore, KYC is also a great source of client dissatisfaction with regular annoyance caused by inexperienced or distracted account managers failing to

complete client on-boarding and periodic reviews in a timely or efficient manner, with particular client irritation caused by confusion and numerous follow-up requests for clarifications, alternative or additional documents etc.

KYC process improvement needs to directly address these cost, efficiency, core, quality and satisfaction issues by so doing, improve risk management, reduce costs and support front office staff in their efforts to concentrate more on revenue generating activity.

Process: Lessons learned

Cost, efficiency, core, quality and satisfaction issues are also common problems in many other business process areas.

With the goal of improving KYC processes, insight can be gained by referring to a number of common IT, engineering and production quality frameworks. These include:

- *CMM* — Capability Maturity Model
- *ITIL* — the Information Technology Infrastructure Library for Service Management
- *COSO and COBIT* — financial and IT control frameworks
- *Lean* (often associated with *The Toyota Way* production model) which helps drive organizational (and process) learning
- *Agile*, an iterative IT development methodology that guarantees the time and the cost and maximises the scope
- *Six-Sigma* — a data driven approach to measurement and defect reduction
- *Balanced Scorecards* — a commonly used strategic performance management (and reporting) approach that usually covers a range of financial, operational, customer and organizational health measurements

It is encouraging to note that according to the Carnegie Mellon Software Engineering Institute (SEI)¹, home to the CMM(I) model, great benefit can be achieved through process improvement. Cost and in-efficiency, non-core, quality and client dissatisfaction issues can all be addressed and mitigated through improved processes.

The KYC maturity model described in this article is intended to serve as a resource and technology agnostic directional roadmap to improved KYC processes.

Levels 1 and 2 — From chaotic to reactive

The KYC maturity model is based on the typical five levels of a standard Capability Maturity Model.

These levels are typically described as Initial, Repeatable, Defined, Managed and Optimized and have very strict meanings. For the purposes of this article, the KYC maturity levels have been somewhat renamed for easier understanding and are depicted below:

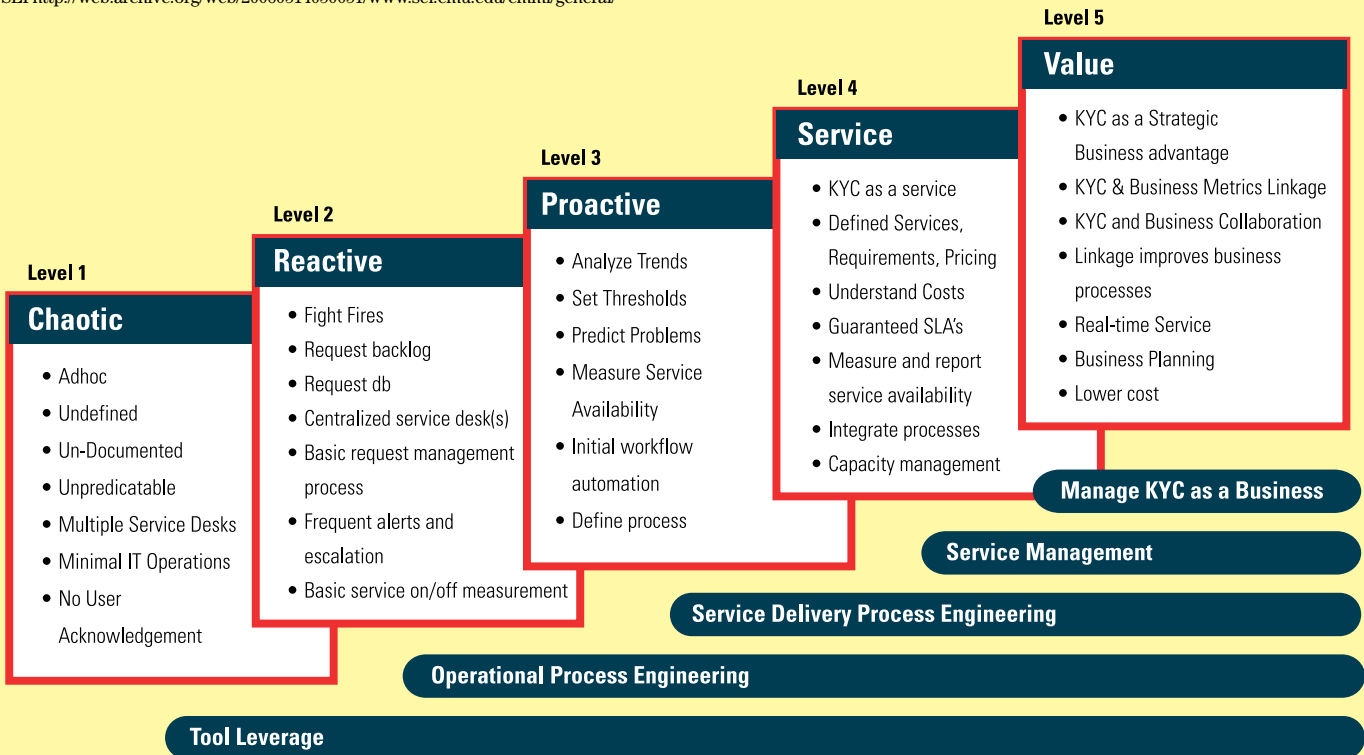
Few organizations would be happy to find themselves at Level 1, the *Chaotic* level. But the one good thing about this level is that the path out of this level is quite clear. The Chaotic attributes — ad-hoc activities,

undefined responsibilities, undocumented processes, unpredictable demand, no central control, little systems support and no formal communication — can all be relatively easily addressed and each small improvement will make a quick and real difference.

One common initial step is to implement a “tool.” While tools can be useful, they are seldom the only answer. Implementing a “tool” in a Chaotic process will usually result in the creation of a large (but, at least now, defined) backlog of work to do and may help to move the process maturity level from chaotic to *Reactive*. But *Reactive* is still rough going — fighting fires, continuous distraction, always running behind the ball.

At some stage, the team needs to really start to think about process definition, engineering and reengineering. Process engineering and reengineering starts with an initial process definition — this can be very basic, but until it is written down or depicted, improvement will be difficult. It is important that all of the various players (the customer, the front-office and the compliance and (front/mid/back-office) KYC analysts) are identified and role-defined and all activities (task assignment and re-assignment, escalation and Quality Assurance checks and review steps, signoff etc.) are identified.

¹ SEI <http://web.archive.org/web/20060514050051/www.sei.cmu.edu/cmmi/general/>



Such a process definition may already exist, but may not be followed; or may be planned for implementation, but without any enforcement mechanism.

Level 3 — Proactive

It is not enough to just DEFINE the process. In order to become *Proactive*, one also needs to ensure that it is being REPEATED and — a big step forward — MEASURED.

Workflow tools can help with enforcing a process — and there are many good workflow tools on the market. While workflow can ensure that a process is being repeated, it is also extremely important that the workflow can support reporting and process inspection and continuous change. Change is, after all, inevitable — and experimentation should be welcomed.

With some level of a defined and improved process in place one can start trying to get ahead of the curve. Now that the process is not only Defined (what you want to happen) but is being Repeated with some degree of regularity and rigor, it can be better Measured.

Six-Sigma

The Six-Sigma methodology can be very helpful in any attempt to effectively and efficiently measure. The Six-Sigma DMAIC methodology with its Define, Measure, Analyze, Improve and Control stages can be mapped to various KYC process touch points and can help drive improvement by uncovering process variances. (See the online version of this paper for more detail).

The process is now Defined, Repeatable and Measured. The process maturity can be said to be Level 3 (Proactive). The defined process is being analyzed, thresholds are being set and some level of predictability is in place.

Level 4 — Service managed

Level 4 (Service Management) takes the defined process and the proactive approach to a whole new level of professionalism. This is where some of the formal *ITIL* principles (for Service Delivery and Management), some *Lean* and *Agile* (process and planning disciplines) lessons and Balanced Scorecard reporting can come in useful. (See the online version of this paper for more detail on *ITIL*, *Lean*, *Agile* and *Balanced Scorecards*).

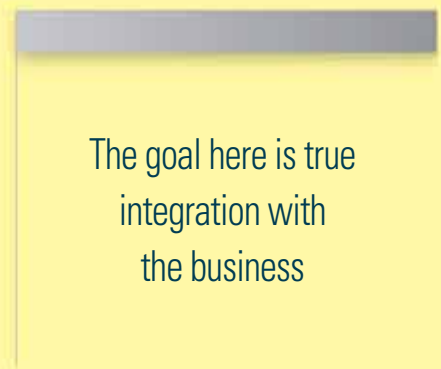
With balanced, lean and agile services agreed and in place, a KYC operation can start to better integrate into other

business processes. The team can also plan to handle peaks in demand by flexing capacity within pre-defined parameters to continue to maximize (prioritized) on-time delivery.

The process improvement journey leads from DEFINED to REPEATABLE and MEASURED and then to PREDICTABLE, PLANNED, BALANCED and PRICED (COSTED). Continued process improvement and optimization over a period can lead to Level 5 — Value Management.

Level 5 — Value management

Level 5 is “managing KYC as a business” — a goal worth aiming for in any other internal or external organization.



The Value Management level is where one has not just identified and minimized the COST of KYC but has also identified, captured and shared the VALUE of KYC — and indeed, created value through KYC.

As part of integrating KYC into other business processes as mentioned earlier, one can look to close the loop on, for example, “commercial information:”

- information of a potentially commercially-actionable nature that is discovered during KYC analysis can be fed back to the master Customer Relationship Management system
- parent tree information, specifically key directors and persons-of-influence can be communicated back as possible new leads, contacts or influencers
- any media-monitoring put in place to trap “significant AML-relevant events” (e.g., M&As, board changes, new business activities) can be widened to also identify commercially-relevant events (e.g., new deals, partnerships, international expansions etc.)

Likewise, one can also try to close the loop on operational risk information, market and product trend information through various business intelligence reports etc.

The goal here is true integration with the business — as fast as the business can handle, as smart as can be managed and as cost-effective as possible.

That’s it, that’s the model. It is intended to be as simple and practical as possible — as a way of quickly identifying one’s current state and as a simple roadmap to further process improvement.

The right mix

Implementing this simple model can be done with a few simple principles in mind — these principles concern the right mix of people, process and technology.

KYC is all about people. Many enhanced due diligence activities cannot be automated — no tool can analyse and verify parent trees, sift through false-positive PEPs and really understand bad press. Only people can do that. People are not cheap and people get distracted. A good resourcing model can maximize morale and limit cost. A professional environment with a focus on experimentation and improvement is also important.

Great processes supported by good technology are important. Not necessarily great technology and good processes, but great processes and good technology. The process should always drive the technology choices. What are great processes? Above all they are capable of Continuous Process Improvement. And what is good technology? Basically, it needs to be “enabling” and open to change. Secure is a must; flexibility should be built in — intuitive is helpful.

Conclusion

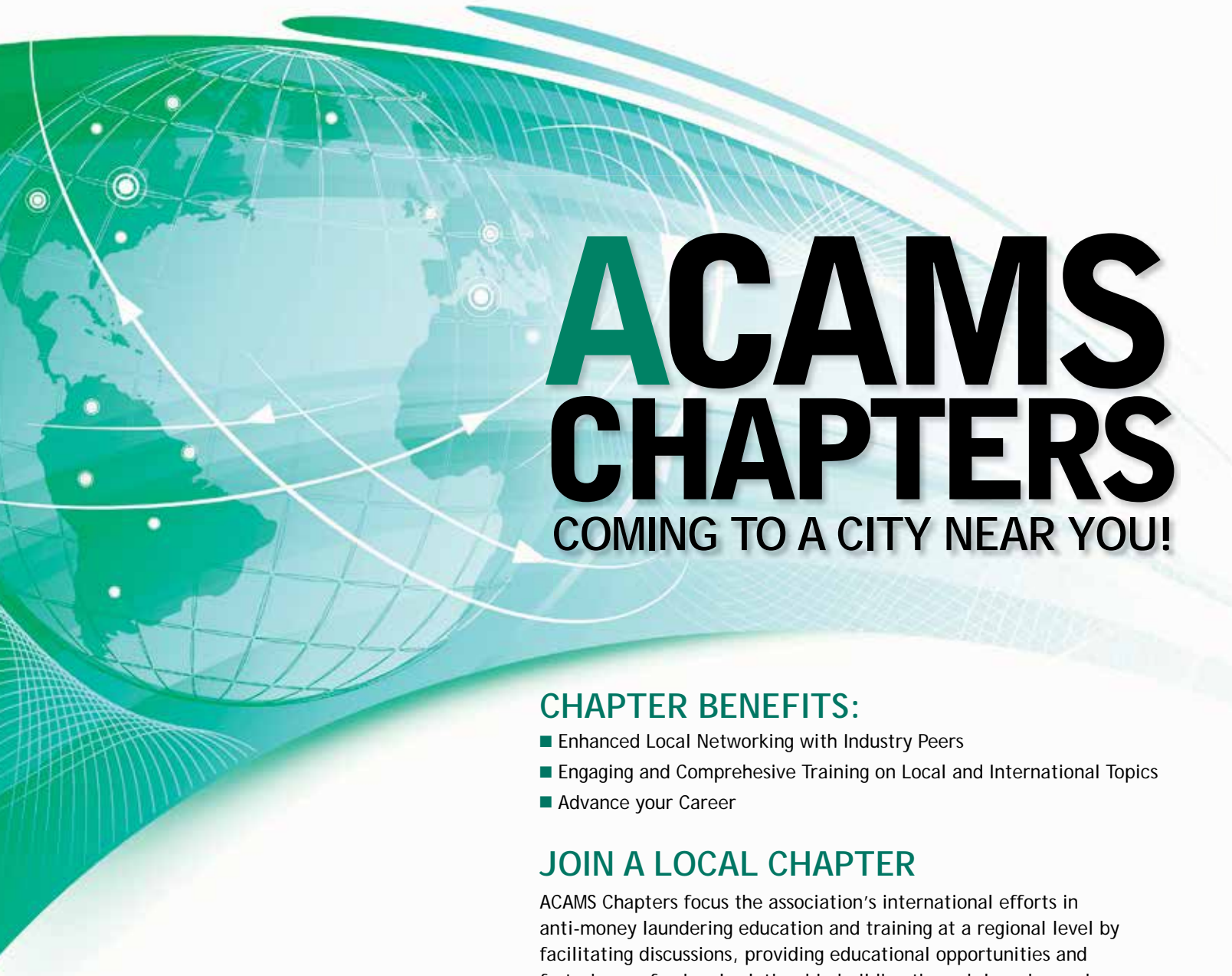
Now, more than ever, KYC is necessary and is growing in importance and in cost. Now is the time to improve our processes, adopt service and business value approaches to KYC to better manage risk, reduce costs and free-up resources to generate more revenue. **A**

Patrick Ryan, co-founder, KYCnet BV, Amsterdam, The Netherlands, patrick-ryan@kycnet.com

An expanded version of this article can be found on www.ACAMSToday.org.

Association of Certified
Anti-Money Laundering
Specialists®

ACAMS®



ACAMS CHAPTERS

COMING TO A CITY NEAR YOU!

CHAPTER BENEFITS:

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

JOIN A LOCAL CHAPTER

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

**TO FIND OR START AN ACAMS
CHAPTER IN YOUR CITY, PLEASE VISIT
THE "ABOUT CHAPTERS" AT**

www2.acams.org/Chapters

Visit us online for more Details!

Enhanced due diligence is a must to mitigate AML exposure in Turkey

The laundering of funds generated from the sale of drugs continues to be a major threat, not least due to the frequent nexus between drug cartels and terrorist organizations. The recent money laundering investigation into HSBC's Mexican operations¹ is a case in point and highlights how financial institutions, despite significant efforts undertaken during past decades, continue to be exposed to the risk of drug cartels laundering money. Turkey, given its major role in facilitating the transfer of illegal drugs to Western European markets, faces significant AML/CFT risks. Because of this risk, it is important to undertake enhanced due diligence when dealing with Turkish clients as part of an effective money laundering mitigation strategy.

A booming economy

Turkey is the world's 17th largest economy and continues to experience significant economic growth. It is also an important and active geopolitical player in the Middle East, by helping ensure that no security threats emerge from neighboring countries such as Iraq and Syria and also from terrorist organizations such as the Kurdistan Workers' Party (PKK). Turkey's geostrategic position also makes it attractive to drug trafficking organizations which use the country as a turntable for dispatching drugs, mostly heroin, to European markets. Turkey's financial intelligence unit (FIU) claims that Turkey continues to serve as a transit route for drug traffickers smuggling an estimated \$5 billion worth of illegal drugs yearly.

Given this background, it is clear why organizations striving to combat money laundering were alarmed when the Turkish government launched an "Amnesty Program for Certain Unrecorded Assets" designed to bolster foreign direct investment from November 2008 to September 2009. As reported in the monthly publication *Executive Magazine*, the Financial Action Task Force (FATF) and the European Union (EU) were critical of the program due to its 'no questions asked' approach and the risk of abuse of the program for money laundering purposes, thereby defeating the purpose of attracting sustainable financial sources.²

Although Turkey's economic and political development have been generally viewed positively, criticism regarding the country's stance toward combating money laundering and terrorism, in particular the latter, continue to challenge the country's relevant institutions. In fact, Turkey is the only European country to have been blacklisted by the FATF as one of the "Countries Not Committed to an Action Plan: High-risk and non-cooperative."

Turkey's efforts to combat money laundering

Although Turkey does not currently meet international AML standards, it appears to have made a stronger commitment to closing the gaps in its AML and CFT regime particularly in 2008, 2011 and 2012.

The most recent FATF Mutual Evaluation Report³ dates back to 2007 and therefore does not include an evaluation of the most

recent developments and efforts undertaken by Turkey, so the main developments are summarized briefly below.

- In September 2008, the Turkish Ministry of Finance passed a directive to tighten Turkish anti-money laundering legislation. "The Directive on the Harmonization Program Regarding Responsibilities Related to the Prevention of the Laundering of Criminal Proceeds and the Financing of Terrorism," requiring all financial institutions to improve the monitoring of financial transactions through the adoption of standardized procedures and an increase in staff training. The directive also mandates the institutions to establish specialized departments to ensure that the appropriate procedures are being followed.
- Most recently in 2011, the Turkish newspaper, *Hurriyet Daily* reported that the Turkish FIU (Financial Crimes Investigation Board — MASAK) was working toward broadening international cooperation to combat money laundering and the financing of terrorism.⁴ According to the article, MASAK cooperates with Indonesia, Portugal, Sweden, Mongolia, Afghanistan, Georgia, Albania, Syria, Romania, Croatia, Macedonia, South Korea, Bosnia Herzegovina, Japan, Ukraine, Norway, Jordan, Senegal, Luxembourg, Britain, Canada, Monaco, Finland and Belarus. MASAK was also in talks with Germany and the United States.
- In March 2012, *Today's Zaman* reported that Ankara signed a memorandum of understanding with the United States to exchange intelligence to dry up the

¹ <http://www.bbc.co.uk/news/world-latin-america-18993476>

² <http://www.executive-magazine.com/getarticle.php?article=12140>

³ <http://www.fatf-gafi.org/countries/s-t/turkey/documents/name,1786,en.html>

⁴ <http://www.hurriyetdailynews.com/default.aspx?pageid=438&n=turkey-seeks-wider-cooperation-against-money-laundering-2011-10-11>



terrorist Kurdistan Workers' Party's (PKK's) financial resources. MASAK would be aided by the relevant U.S. authorities to tighten its grip over the ways the terrorist group makes money to procure arms to be used in its violent campaign in the country.

Turkey views the listing as unfair because MASAK has made significant strides in combating the financing of terrorists and money laundering. Turkey, through MASAK, has signed a number of bilateral agreements with a number of other countries.

Kurdistan Workers' Party (PKK)

The Kurdistan Workers' Party, which is commonly known as PKK, is listed as a terrorist organization by Turkey, the EU, Australia and the United States amongst others. It has been fighting an armed struggle against the Turkish state for an autonomous Kurdistan and greater cultural and political rights for the Kurds in Turkey. Turkey labeled the organization as an ethnic secessionist

organization that uses terrorism and the threat of force against both civilian and military targets for the purpose of achieving its political goal.⁵

According to the web site of the Australian government,⁶ the PKK was formally established by Abdullah Ocalan in 1978. The organization adopted a communist ideology, but from its inception was primarily committed to the creation of an independent Kurdish state in south-eastern Turkey. After the end of Cold War, the PKK increasingly emphasized its role as a Kurdish nationalist movement. At times the group has sought to increase its popularity by exploiting the religious sentiment of the Kurdish community, but the organization was and remains predominantly secular.

The PKK acquires the largest amount of its funding from drug trafficking, which some commentators have claimed garnered as much as 500 million Euros (800 million U.S. dollars) for the organization in 2008. At different times, the PKK has reportedly

controlled up to 80 percent of the European illicit drug market. In June 2008, in recognition of its involvement in these activities, the U.S. State Department added the PKK to its list of major international drug-dealers under the Foreign Narcotics Kingpin Designation Act. Other criminal activities that contribute to the PKK's finances include: human trafficking, money laundering and prostitution rackets. Revenue is also raised by collecting 'taxes' — through voluntary means or coercion — from Kurdish diaspora communities around the world. In 2007, the group reportedly raised approximately 12 to 15 million dollars in Europe alone through commercial activities (including semi-legitimate activities) and donations. Sales of publications, grants, aid campaigns and revenues obtained from 'special nights' organized by PKK branches in Europe also contribute to the group's coffers.⁷

The PKK is also known as: Freedom and Democratic Congress of Kurdistan, HPG, KADEK, KG, KHK, Kongra Gel, Kongra

⁵ http://travel.state.gov/travel/cis_pa_tw/cis/cis_1046.html

⁶ <http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/28B052FC3CCE4009CA2570DF000FB458?OpenDocument>

⁷ <http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/28B052FC3CCE4009CA2570DF000FB458?OpenDocument>

Gele Kurdistan, Kurdish Freedom Falcons, Kurdish Liberation Hawks, Kurdistan Freedom and Democracy Congress, Kurdistan Freedom Brigade, Kurdistan Freedom Hawks, Kurdistan Halk Kongresi, Kurdistan Labor Party, Kurdistan Ozgurluk Sahinleri, Kurdistan Peoples Congress, New PKK, Partiya Karkeren Kurdistan, Peoples Congress of Kurdistan, People's Defence Force, TAK, Teyrbazên Azadiya Kurdistan.

Halkbank's links to Iran

It is worth noting that although Turkey's banks, apart from the state-owned Halkbank, have stopped doing business with Iran amid tightening sanctions from the United States and the European Union as reported in the *Wall Street Journal* in February 2012. Halkbank's main business with Tehran, the report said, is handling payments from Turkey's sole refiner, Tupras, which is owned by the country's largest conglomerate, Koc Holding. The article further claims, that Halkbank has also handled business for Indian refiners unable to pay Tehran for imported oil through their own banking system for fear of angering the United States. A *Wall Street Journal* profile of the bank, known as People's Bank, details

the negligible nature of the Iran business, which contributed less than 1 percent of the bank's fourth-quarter profits.⁸


Enhanced due diligence required

The UK regulatory Financial Services Authority (FSA) "advises all financial institutions and other persons regulated for anti-money laundering purposes to consider applying increased scrutiny to transactions" associated with Turkey amongst others, including by conducting enhanced due diligence and ongoing monitoring.⁹ It is also important within this context to assess the links and nature of relationships between companies and individuals across borders and set within the political context of an increasingly powerful geopolitical player in the Middle East and North Africa (MENA) region.

Conclusion

The FATF has acknowledged high levels of political commitment on the part of the Turkish government toward addressing strategic AML/CFT deficiencies. Despite these continuous efforts however, Turkey remains

on the FATF's list of countries that have not made sufficient progress in addressing deficiencies identified. The FATF has been more critical of Turkey's efforts to combat terrorism and has suggested that Turkey should focus on adequately criminalizing terrorist financing and implementing an adequate legal framework for identifying and freezing terrorist assets.

Beyond this, the activities of the PKK terrorist organization, in particular in the context of the current Syrian conflict,¹⁰ as well as the fact that around 80 percent of the heroin dispatched to Europe passes through Turkey from Afghanistan, combined with the weaknesses in the country's AML/CFT regime, underline the high money laundering risks to which institutions undertaking business in Turkey can potentially be exposed to, and make it clear that undertaking enhanced due diligence is the only way to mitigate the risk of being used as a conduit for criminal or terrorist activities.¹¹ 

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

⁸ <http://blogs.wsj.com/corruption-currents/2012/02/21/state-owned-turkish-bank-continues-iran-deals/>
⁹ http://www.hm-treasury.gov.uk/d/financial_sector_advisory_mar2012.pdf
¹⁰ <http://www.reuters.com/article/2012/07/27/us-turkey-syria-idUSBRE86Q11Y20120727>
¹¹ http://www.huffingtonpost.co.uk/2011/07/31/turkeys-membership-of-eu-_n_914466.html

When You Need to Say Compliance, You Need to Say it Right.

Getting organization-wide support from critical business units is always a challenge for the Financial Compliance Professional. Good compliance communications is the key. Poor communications can weaken internal support and invite regulatory and legal consequences.

With decades of relevant and tested knowledge, expertise and experience, the *ComplianceComm* team can help you overcome obstacles and resolve compliance issues through better communications. We don't provide off-the-shelf, one-size fits all solution sets. Your challenges, your audiences, your situations are unique to your organization. So are our solutions.

Compliance
Comm

A division of CorpComm Solutions, LLC
 solutions@compliancecomm.com
 703.297.7458

**FINANCIAL REPORTING LAWS ARE THE RULE...
 INEFFECTIVE COMMUNICATIONS IS THE ROADBLOCK...**
ComplianceComm is the Remedy

See our **SARSnSTRIPS**® Cartoon in **ACAMS Today**
 Want one of your own?
 Singles and subscriptions available.



Protect your organization from a world full of risk.

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

Don't blink

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

LexisNexis® Risk Solutions understands the nature of risk and delivers AML/compliance, risk mitigation and enhanced due diligence solutions to help you proactively manage it. Solutions such as LexisNexis® Bridger Insight™ XG which is specifically designed to help you conduct due diligence, comply with global regulations and reduce identity fraud risks efficiently and cost effectively—all through a single platform. It's one reason a majority of the top 25 U.S. banks trust LexisNexis Risk Solutions.

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

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

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



Now serving the Asia market
through our Hong Kong office—
www.lexisnexis.com.hk

Request your free 30-day trial*
of Bridger Insight XG today at
lexisnexis.com/risk/freetrial

Risk Solutions
Financial Services

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Bridger Insight is a trademark of LexisNexis Risk Solutions Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2012 LexisNexis. All rights reserved.

The AML/CFT enforcement regime in South Africa



The Financial Intelligence Centre (the FIC) is South Africa's Financial Intelligence Unit (FIU) mandated to establish an anti-money laundering and counter terror-financing regulation regime in terms of the Financial Intelligence Centre Act No. 38 of 2001, (the FIC Act), as amended.

Various compliance obligations have been introduced in terms of the FIC Act to enable the protection of institutions against exploitation by criminals and terror financing networks. In the execution of its mandate, the FIC Act requires all businesses to report suspicious and unusual transactions to the FIC and defines the anti-money laundering responsibilities of specific categories of business (called accountable institutions) as well as the supervisory bodies which have oversight over them.

The FIC Act imposes obligations on accountable institutions regarding client identification, recordkeeping and reporting duties, as well as the implementation of internal compliance structures and policies.

South Africa is the only African member of the international anti-money laundering standard-setting body, the Financial Action Task Force (FATF). Regionally, South Africa is a participant in the 14-member Eastern and Southern Africa Anti-Money Laundering Group and is also a member of the Egmont Group which is an international organization consisting of 120 FIUs. With the receipt, analysis and dissemination of financial intelligence by the FIC to relevant local and international authorities, South Africa is able to participate in global efforts in the identification of activities involving transnational organized crime, including fraud, smuggling, human trafficking, the narcotics trade and the stripping of the country's natural resources.

To enhance the effectiveness of the FIC in carrying out its mandate, various amendments to the FIC Act came into operation on December 1, 2010. The main objective of these amendments was to provide for an administrative enforcement framework within which administrative sanctions under the FIC Act could be applied. The key features of the administrative enforcement framework are:

- (i) To extend the powers and functions of the FIC to enhance supervision and enforcement of compliance with the Act in a coordinated and integrated manner together with supervisory bodies, and to fulfill the responsibilities of a supervisory body where these do not exist;
- (ii) To clearly express the mandate of supervisory bodies to supervise and enforce compliance with the obligations on accountable institutions regulated by them under the FIC Act;
- (iii) To empower the FIC and supervisors to undertake inspections, issue directives, request information, impose administrative sanctions and apply to the courts for an interdict or a writ of mandamus, where appropriate;
- (iv) To ensure consistency in the enforcement powers afforded to supervisors;
- (v) To enhance cooperation and sharing of information between the FIC, supervisors and law enforcement agencies;
- (vi) To create an appeal mechanism against decisions of the FIC or supervisors; and
- (vii) To provide for every accountable institution and every reporting institution to register with the FIC.

Supervisory bodies perform the core function of supervising and enforcing compliance over accountable institutions. For example, the Estate Agency Affairs Board is responsible for enforcing FIC Act compliance obligations relating to estate agents.

The FIC and each of the respective supervisory bodies are expected to work together to coordinate their approach and ensure that the requirements of the FIC Act are being fulfilled and that there is consistent application. A memorandum of understanding is entered into between the FIC and each supervisory body to give effect to this. In terms of this coordinated approach, each supervisory body exercises primary responsibility for supervision and enforcement in relation to their licensed entities in terms of the FIC Act.

There are two exceptions to the supervisory body role, in which the FIC takes prime responsibility, namely:

- Registration with the FIC;
- Reporting to the FIC by the various accountable and reportable institutions.


Supervisory bodies are empowered to conduct inspections on their individual licensed accountable institutions to determine compliance with the FIC Act. Section 45(B) of the FIC Act provides for joint inspections in which a supervisory body and the FIC can collaborate. It is preferable for the FIC to accompany supervisory bodies on inspections to ensure that information is shared regarding the inspections as well as their outcome. Such collaboration also ensures a consistent approach to inspections and the interpretation of the FIC Act. Supervisory bodies can also be advised by the FIC on possible actions which can be taken as a result of the inspection findings.

Where there is no supervisory body in place and an accountable or reporting institution is found to be non-compliant with the FIC Act, the FIC has the power to impose a sanction. The authority to issue a sanction rests with the director of the FIC. Where there is a supervisory body, sanctions will be imposed by the head of the supervisory body in consultation with the FIC. A sanction could take the form of a caution, reprimand, a directive to take remedial action, or to make specified arrangements, the suspension of certain business activities, and a financial penalty. Natural persons can also be sanctioned when necessary.

The financial penalty that may be imposed is one not exceeding R10,000,000.00 in respect of natural persons and R50,000,000.00 in respect of legal persons. Criminal liability is dependent on the type of offense committed and could result in imprisonment for a period not exceeding 15 years or to a fine not exceeding R100,000,000.00. Where less severe offenses have been committed, imprisonment for a period not exceeding five years or a fine not exceeding R10,000,000.00 is permissible.

The introduction of these amendments has empowered the FIC in carrying out its mandate

A natural or legal person has a right to appeal a sanction. The appeal is done under the auspices of Section 45(D) of the FIC Act. The lodging of a notice of appeal must be done within 30 days of the aggrieved party receiving notice of the sanction. Once the hearing of the appeal has taken place, the Appeal Board will announce its decision in writing to confirm, set aside or vary its initial decision. The Appeal Board could also direct the matter back to the FIC or supervisory body for consideration.

The introduction of these amendments has empowered the FIC in carrying out its mandate and has broadened the extent to which the FIC can take effective action against non-compliant accountable or reportable institutions. This strengthens the FIC's compliance enforcement capability and promises greater success in the battle against money laundering and terror financing on both the domestic and international fronts. 

Christopher Malan, senior manager: compliance and prevention, The Financial Intelligence Centre, South Africa, communications@fic.gov.za

How banking institutions in Japan should react to the FATCA Account Identification Regulations

Industry organizations in each country submitted comment letters toward the proposed regulations on U.S. Foreign Account Tax Compliance Act (FATCA), which was released on February 8, 2012. The comments seem to indicate that financial institutions are hesitant to commence their action for FATCA given the demands by the Internal Revenue Service (IRS) to design institutional arrangements and to clarify the details described in their comments letters. A joint statement from the United States and five European countries; France, Germany, Italy, Spain, and the United Kingdom, were released simultaneously with the Proposed Regulations and the draft of the Japanese government statement have not specified exact timelines. It is unclear that such inter-governmental agreements would be effective prior to FATCA implementation deadlines. But the intergovernmental agreements has been characterized as “remarkable progress” in a comment letter by the Japanese Bankers Association, as these agreements would clear most of the current legal restrictions for compliance with FATCA. Repeal of the obligation on withholding recalcitrant account closures shall make reaction of FATCA a more realistic issue for foreign financial institutions (FFIs). There are four categories of classifications in FATCA:

- 1) Identification of entity that must comply with FATCA;
- 2) Identification of account; both current and new;
- 3) Reporting; and
- 4) Withholding.

The following is a recommended course of action for identification of accounts; current and new, which FFIs are able to initiate at this moment as an answer to the question: “What should FFIs tackle right now?”

New account opening procedure under terms of the Revised Act on Prevention of Transfer of Criminal Proceeds (Revised Act)

The demand to minimize chaos at the business scene by simultaneous parallel consideration on KYC for compliance to both the Revised Act and FATCA was well known before the release of the proposed regulations. The proposed regulations focus on AML/KYC procedures; and seem to have some consideration to minimize chaos caused by requirements under the Revised Act; however, KYC procedures for FATCA might be substantively added to the current AML/KYC process. We would interpret that FFIs can rely on AML/KYC procedures required in FATF-compliant countries and have to implement detailed rules on KYC; including the document to be obtained outlined in the proposed regulation. In their comment letter the Japanese Bankers Association indicated they would like confirmation and clarification that financial institutions can just rely on AML/KYC procedures and that there is no need of additional FATCA KYC processes needed. Therefore, we recommend that you closely monitor development of the following six items mentioned in the comment letter, acknowledging the difference between the Revised Act and FATCA.

- 1) Types and scopes of documentary evidence

- 2) Expiration period of documentary evidence and procedures to renew the identification process
- 3) Timing of identification,
- 4) Transactions subject to identification procedures (financial accounts)
- 5) Obligation to retain a copy of documentary evidence
- 6) Standard for identification of U.S. substantial owners

Clarification of the range to be aggregated

Aggregation by each account holder is needed on the premise of certain threshold usage on account KYC procedures. The proposed regulation states that aggregation “to the extent that the FFI’s computerized systems link the accounts by reference to a data element such as client number or taxpayer identification number” is acceptable. Therefore, when a customer is assigned a different client number by each branch, those accounts cannot be aggregated under such a requirement. Meanwhile most of Japanese banks accommodated such an aggregation when they implemented “payoff,” which means only a deposit of JPY 10,000,000 and its interest shall be protected under the Japanese Deposit Insurance Act, but accounts subject to aggregation are limited. FATCA covers accounts, which are not applicable to payoff rule; such as foreign currency deposits. FFIs have to confirm additional measures when they may not establish a system to conduct aggregation of same client number.

Procedures to conduct electronic research on U.S. Indicia of a preexisting individual account

The KYC process for individual accounts in the proposed regulations require FFIs to search information to indicate if the account holder is a U.S. person, hereinafter referred to as US indicia, in accordance with certain search conditions. However, such information searches would not produce any result, under the current system of KYC procedures and client data input and database maintenance. In such a case, there is a method to document certification of no extraction results instead of searching. When the above mentioned documentation process is troublesome for FFIs, they may arrange extraction conditions, conduct a search and keep a record of no results.

FFIs can further enhance their search results by paying attention to client accounts with standing instructions or periodic fund transfer instructions. There would be various methods to input data and to maintain a database of such instructions for example, some FFIs can directly conduct their search of periodic fund transfer instructions data while others can search fund transfer data in their transaction records with the transaction records being linked to the account. Therefore, FFIs are required to sufficiently perform a feasibility study prior to actual screening and implementation of the search/screening policies.

In addition, the Japanese Bankers Association's comment letter highlighted the clarification of the definition of standing instruction, which demands that only frequent and large amount fund transfers should be regarded as U.S. Indicia. If this comment is reflected in the finalized regulation and extraction results are narrowed down, it is possible for FFIs to decrease their procedures after conducting a client account review. In this case, FFIs need to evaluate the frequency and the amount in their extraction condition.

Targeted information on customer database

Copies of passport and drivers licenses which are acquired as paper-based identification and stored electronically do not seem to be required to be included in the screening process. The proposed regulation defines "electronically searchable information" as information that an FFI maintains in its tax reporting files, customer master files, or

similar files, and therefore, is stored in the form of an electronic database against which standard queries in programming languages, such as Structured Query Language, may be used. Information, data or files are not electronically searchable merely because they are stored in an image retrieval system, such as portable document format (PDF) or scanned documents. Furthermore, FFIs who have outsourced overseas remittance operations only need to search their own database, although there is an issue to what extent do they maintain data related with remittance upon receiving such applications from clients.

Identification of certain insurance product types

The proposed regulations exclude insurance contracts that provide pure insurance protection, such as term life, disability, health, and property and casualty insurance contracts, from the definition of a financial account. These contracts are not required to be examined. However, funding insurance policies that provide coverage against damage but also savings-based do not seem to fall under the category of pure insurance protection. The definition of term life insurance in FATCA is a contract in which equal periodic premiums are payable annually or more frequently during the period of the contract and single premium life insurance does not equate to term life insurance. Accordingly, FFIs need to consider the premium payment frequency to determine their examination coverage.

Holder of the insurance account


FFIs are required to pay attention to whether the contract holder or the beneficiary should be regarded as holder of the account. The proposed regulations set forth that an insurance or annuity contract that is a financial account is treated as held by the contract holder if such person can access cash value of the contract, for example, through a loan, withdrawal, or surrender, or change a beneficiary under the contract. However, if the contract holder cannot access cash value or change a beneficiary then the contract is treated as held by each beneficiary under the contract. Therefore, in most instances for Japanese insurance companies, the contract holders are treated as holders of the account. But once the amount of reimbursement is fixed at contractual maturity, the holder of the account would be changed from contract

holder to the beneficiary in accordance with the contract. FFIs have to revise KYC procedures on beneficiary of maturity repayment to be compliant with FATCA.

Formulation of process and internal control cover internal validation

The proposed regulations require the FFI to conduct periodic reviews of its compliance with FATCA policies and procedures. The responsible officer of the FFI must periodically certify to the IRS compliance with FATCA requirements. FFIs are further required to record their execution processes and results of KYC procedures for subsequent validation to conform with the requirement. To satisfy this requirement, FFIs might apply a pilot method through which the FFIs only conduct identification of U.S. account ad referendum — taking no account of ex post facto validation — and putting the procedures to be conducted in writing prior to full-scale implementation. After full-scale implementation, execution results could be documented more easily in accordance with the written procedures, which might be a more efficient way than targeting ex post facto validation at one time.

Conclusion

This covers the common issues, with or without intergovernmental agreement, for both participating FFIs and registered deemed-compliant FFIs to conduct further analysis regarding their compliance with pending FATCA implementation. However, even registered deemed-compliant FFIs need to keep in mind that they have a shorter period of time remaining because they are required to complete their implementation policy to preclude non-resident U.S. person and identification of preexisting account by July 1, 2013. It is also necessary to tackle the FATCA timeline by watching further development of intergovernmental agreements, public announcements of additional guidance, and the finalization of the Proposed Regulations. 

Masahiko Okamoto, senior partner, Ernst & Young ShinNihon LLC, okamoto-mshk@shinnihon.or.jp

Contributor: Hue Dang, CAMS, head of Asia, ACAMS, hdang@acams.org

動き出したFATCA にどう対応すべきか-口座特定



前文

2012年2月8日に公表された米国の外国口座税務コンプライアンス法(以下、「FATCA」という)の規則案に対するコメントレーターが各国の業界団体より提出されました。コメントレーターに記載されたIRSへの制度設計に対する要望事項や各論の明確化の要望を鑑みれば、個々の金融機関は、現時点でFATCA対応を開始することに躊躇するかもしれません。また規則案と同時に公表された欧州5か国と米国の共同声明や一部報道機関から報道された日本政府案にタイムラインが明示されていないため、政府間協定がFATCA施行前に決着するのか不明瞭です。しかし、全銀協のコメントレーターに「大きな第一歩」と記される通り、これらの政府間協定が実現すればFATCAを遵守するうえでの法務上の制約の多くは取り除かれると思われる。特に源泉徴収の撤廃、非協力口座に対する口座閉鎖の撤廃が実現することにより、非現実的だったFATCA対応を現実の問題として捉えることができると考えられます。

本稿では、今金融機関は何をすべきかという問いに対する回答として、①FATCA対応すべきエンティティの特定、②口座特定(既存・新規)、③報告、④源泉徴収、と4つに分類されるFATCA対応のうち、現時点で対応を開始することが可能な②口座特定(既存・新規)に絞ってその対応方法に関するエッセンスを提供します。

新規口座開設手続 — 改正犯罪収益移転防止法(以下、「改正犯収法」という)との関連

規則案の公表以前より、本人確認手続に関して改正犯収法への対応とFATCAへの対応は同時並行して検討することで、現場の混乱を最小限に抑える必要

性があることが知られていました。今般の規則案は、AML/KYC手続(日本においては犯収法)との関連を示しており、実務の負担を最小限にするための配慮があるようにも見えます。しかし、規則案はFATF遵守国において要求されるAML/KYC手続への依拠を原則としつつ、一方で本人確認手続に関する詳細なルール(例えば、入手すべき書面の例)を定めることで、FATCA用の本人確認手続をAML/KYC手続に追加することを実質的に要求しているように読み取れます。本件に関して、全銀協はコメントレーターにおいて、AML/KYC手続への依拠で足りる、つまりFATCA用の本人確認手続をAML/KYC手続に追加する必要がないことの確認および明確化を要望しています。そこで、新規口座開設手続に関するFATCA対応を進めるに当たり、コメントレーターに記載されている6つの事項(①本人確認資料の種類と範囲、②本人確認書類の有効期限と再確認、③本人確認のタイミング、④本人確認の対象となる取引、⑤本人確認資料コピーの保管義務、⑥実質的米国保有者確認基準)に関して、改正犯収法とFATCAの違いを認識し、改正犯収法に沿って対応したうえで、今後の動向を注視する必要があります。

名寄せ実施可能範囲の特定

口座特定手続において、一定の閾値を用いる前提として、口座保有者ごとの名寄せが必要になります。規則案に「顧客番号やTIN等を通じてコンピューターシステム上名寄せできる範囲で許容する」とあるため、例えば支店ごとに異なる顧客番号を付している等の場合、同一人であったとしても、顧客番号ごとの名寄せで許容されることとなります。一方、銀行はペイオフ導入時に名寄せ対応を行っていると思われませんが、ペイオフ対象は限定的であ

り、FATCAにおいて名寄せすべき対象の口座は外貨預金等のペイオフ対象外の取引も含むため、同一顧客番号の顧客に関して必ずしも名寄せが実施できる態勢にはないかもしれません。そこで、同一顧客番号の顧客に関して名寄せを実施するための追加的な措置を確認する必要があります。

既存個人口座の米国示唆情報に関する電子検索の実施方法

規則案は、個人口座の特定において、データベース(以下、「DB」という)の中に米国人であることを示唆する情報(以下、「米国示唆情報」という)を一定の抽出要件に沿って検索することを要求しています。しかし、現状の本人確認手続、それに伴うデータ入力およびDBの保持の状態より、いくつかの要件に関しては、検索を実施するまでもなく、要件に該当する抽出結果がゼロという場合もあると思われる。その場合、検索を実施せず、要件に該当する抽出結果がゼロであることを証明する書面を残すという方法があります。一方、そのような証明を行うための書面を残すほうがむしろ煩雑である場合、検索条件を整えて、実際に検索を実施し、その結果(つまり抽出結果ゼロ)を残すほうが簡便かもしれません。

一定の抽出要件のうち、スタンディング・インストラクション(定期的な資金移動指図契約)は注意が必要です。定期的な資金移動指図契約のデータを検索できるのか、過去の送金データから検索するのか、口座と紐づけられるのか、いずれも銀行ごとに様々な方法で入力および保持されていると考えられます。そこで、実際に検索を行う前に十分な初期的調査を行った上、検索方針を策定し実行する必要があります。なお、全銀協のコメントレーターにおいて、スタンディング・インストラクシ

まで保有しているのかといった論点もありますが、あくまで自社のDBのみ検索を行えば良いと考えられます。

保険業 - 精査の対象となる保険種類の特定

純粹な保障性の商品(定期生命保険、傷害保険、健康保険、損害保険など)については、金融口座の定義から除外されているため、精査の対象外とします。ただし、損害保険であっても貯蓄性のある積立保険等については、純粹な保障性商品に該当しないと考えられます。なお、FATCA上の定期生命保険の定義は、年払い以上の頻度(年払い、月払い等)で定額の保険料を契約者が支払う契約とされているため、一時払の契約はFATCA上の定期生命保険には該当しません。従って、精査対象の判定において払込方法に留意する必要があります。

保険業 - 口座保有者

保険契約は、契約者と保険金等受取人のいずれを口座保有者として取り扱うかに留意が必要です。キャッシュバリューのある保険契約及び年金契約の口座保有者は、キャッシュバリューの受取人や保険金等受取人を変更する事ができる人、そのような人がいない場合には保険金等受取人が口座保有者と定められています。従って、日本の保険会社では通常は契約者が口座保有者として特定されます。ただし、契約満期時に返戻金が確定した段階では、口座保有者は、その定義に従って契約者から満期返戻金の受取人に変更されるので、満期返戻金の受取人の本人確認手続がFATCAに遵守するように見直す必要があります。

内部検証を視野に入れたプロセスと内部統制の構築-パイロット方式の活用

規則案は、FATCA対応の方針及び手続の文書化とその遵守を定期的に内部検証すること、及び担当役員が一定の証明書を定期的にIRSに提出することを要求しています。この要求事項に対応するために、事後的に検証可能な状態を保持することに留意して口座特定手続を実施する必要があります。これを実現するために、パイロット方式を採用する場合があります。パイロットでは事後的な検証可能な状態は無視して、米国口座の特定のみを暫定的に実施し、本番を実施する前に実施すべき手続を首尾一貫した文書とし、それに従って本番を実施することで、実施結果も容易に文書化することが可能となります。1回で事後的に検証可能な状態を保持することを目指すよりも結果として効率的な方法になると考えます。

最後に

上記の議論は政府間協定の有無にかかわらず生じる共通の論点であり、参加FFIと登録型みなし遵守FFIの双方が検討すべき課題です。ただし、登録型みなし遵守FFIは非居住の米国人を排除するポリシーの導入や既存口座の口座特定等を来年の7月1日までに完了する必要があるため、参加FFIよりも残された時間は少ないことにご留意ください。また、今後の政府案の動向、追加ガイダンスの公表、規則案の最終化を睨みつつ、すでに定められている期限への対応を行う必要があります。本稿がFATCA対応の検討の一助になれば幸いです。 **AI**

新日本有限責任監査法人
金融部 シニアパートナー 丘本 正彦

ョンの定義の明確化が取り上げられています。多額かつ多頻度の送金のみを米国示唆情報と認識すべきという要望です。このコメントレーターが最終規則に反映される場合、検索結果が絞り込まれるので、検索後の手続を減少させることが可能となります。その代り、検索時において、頻度や金額を検索対象とすることに留意が必要です。

DB上で検索対象とする情報

規則案において、「電子的に検索可能な情報」は「税務申告ファイル、または顧客マスター、或いは類似のファイルの中に管理している情報で、電子DBの形式で保存されており、SQL等のプログラム言語を用いて標準的な照会機能が使用できる情報を意味している」、「情報、データまたはファイルは、(PDFファイルやスキャンされた文書等の形式で)画像検索システムに保存されたというだけでは、電子的に検索可能とはならない」と定義されている事から考えると、紙ベースで取得しスキャンで電子的に保存したパスポート、免許証のコピーについては検索不要と考えられます。また、海外送金業務をメガバンクにアウトソースしている金融機関の場合、自社で受け付けた送金関連のデータをどこ

Now with Country Profiles!

Get an at-a-glance overview of the state of anti-money laundering in various countries.

Individual profiles with the latest country specific information:

- ☞ Important facts
- ☞ Instant access to key legislative and regulatory documents
- ☞ Country ratings by international watchdog groups, including the FATF, Transparency International and the Basel Group

More country profiles being added weekly!
Visit moneylaundering.com for details.



Michael Vasquez

Operations Department

Michael Vasquez serves as the operations director for ACAMS. He has been with the organization for over two years and oversees the customer service, IT and fulfillment departments.

Prior to joining ACAMS, Vasquez served as a business consultant and provided operational, financial and vendor contracting guidance to fortune 1000 companies in the Miami-Dade area. He also worked in different operational roles in the travel and healthcare industry where he acquired ample experience in business strategy and growth.

Since joining ACAMS, Vasquez has developed a strategic roadmap to achieve operational excellence with a strong emphasis on member satisfaction. His ultimate goal is to ensure that the ACAMS' membership experience is globally recognized for its excellence.

ACAMS Today: What led you to a career in operations?

Michael Vasquez: For me, it was changes in the working environment. As budgets tighten in companies across the globe, workers with a single skillset become obsolete (e.g., you can no longer just be the customer service guy and not know how your backend systems work so you need to brush up on your IT skills). In short, to stay competitive you have to keep expanding your knowledge and it is this driving force that made me go from a call center professional to an overall operations expert.

AT: What makes your experience working with ACAMS different from your work with other organizations?

MV: It is a niche market. Previously I worked in mass consumption products, open to everyone such as health insurance. ACAMS does not market to the masses thus making it very exclusive and unique.

AT: What steps has your department implemented to make the ACAMS membership experience more rewarding?

MV: How much time and space do we have? Well, here are a few of the steps we have taken: 1) We updated our IT infrastructure to increase the performance of our web sites; 2) We have upgraded and outsourced our printing efforts so membership materials are delivered in a timelier manner; 3) We have streamlined the certification process to avoid delays in application processing; 4) We have upgraded our phone system and 5) staffed our call center accordingly to ensure we do not miss any calls from our members.

AT: What is your favorite membership benefit?

MV: ACAMSToday.org is currently my favorite; however, I will have a new favorite soon but it is still in the works. Stay tuned!

AT: Where do you see ACAMS in five years?

MV: ACAMS is and will continue to be the global leader in its field. I see us expanding our membership base internationally and more importantly expanding the different areas of financial crime which we fight against and cover in our publications and training. I have no doubt that ACAMS will remain the place where everyone comes for their information and training. **FA**

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



SAVE THE DATES!



ACAMS® | MONEY
LAUNDERING.COM®

18TH ANNUAL INTERNATIONAL

AML & FINANCIAL CRIME CONFERENCE

Pre-Conference Workshops
CAMS Examination Preparation Seminar
MARCH 17, 2013

Main Conference
MARCH 18-20, 2013

**ACAMS Members now receive special rates!
Plus SAVE \$350***

when you register and pay by October 19, 2012, with VIP code AD-350.

Visit moneylaunderingconference.com

Call: +1 305.373.0020

Email: info@acams.org

*Register and pay by October 19, 2012, and save \$350 off the main conference standard price for ACAMS members. Pre- and post-conference workshops are not included in main conference pricing. Please be sure to mention VIP code AD-350. Discounted rates are available for government, small institutions and groups of 3 or more. Please contact Geoffrey Fone at gfone@acams.org or at +1 786.871.3021 for details. Discounts cannot be combined.

International Identity Verification Made Easy

One Platform – One Integration – 30+ Countries – Over 2 Billion Records

