EDICIÓN ESPECIAL 10° ANIVERSARIO

ACAMS® TODAY

La Revista Para los Profesionales en el Campo Antilavado de Dinero

Los 10 mejores consejos sobre ciber-concientización para el profesional ALD 48

Retrospectiva: 10 años de ACAMS 14

SEPTIEMBRE–NOVIEMBRE 2011
VOL. 10 NO. 4

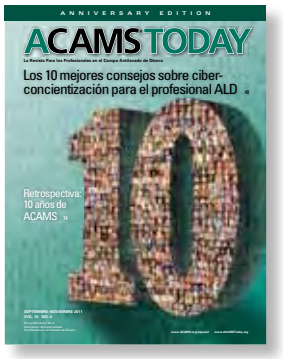
Una publicación de la
Asociación de Especialistas
Certificados en Antilavado de Dinero

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

Asociación de Especialistas Certificados en Antilavado de Dinero®
ACAMS®

ACAMS TODAY

EN LA PORTADA



Los 10 mejores consejos sobre ciber-concientización para el profesional ALD

48

ACAMS Today está diseñada para brindar información exacta y acreditada referida a los controles internacionales de lavado de dinero y los temas relacionados con los mismos. Al realizar esta publicación, ni los autores ni la asociación están realizando servicios legales u otros servicios profesionales. Si se requiriera tal asistencia, deberán obtenerse los servicios de un profesional competente.

ACAMS Today es publicada cuatro veces al año para los miembros de ACAMS.

Para asociarse o publicar anuncios publicitarios, contactar a:
ACAMS
Brickell Bayview Center
80 Southwest 8th Street, Suite 2350
Miami, FL 33130, EE.UU.

Tel. 1-866-459-CAMS (2267) ó
1-305-373-0020
Fax 1-305-373-5229 ó
1-305-373-7788

E-mail: info@acams.org
Internet: www.ACAMS.org
www.ACAMS.org/espanol

EN ESTA EDICIÓN

DE LA EDITORA

¡Feliz décimo aniversario y felicitaciones a todos los miembros que han contribuido a los diez exitosos años de ACAMS en la actividad!

No es ningún secreto que soy una fanática de los deportes. Me gusta especialmente mirar la gimnasia. A medida que iba creciendo, esperaba ansiosamente cada cuatro años la nueva edición de las Olimpíadas de verano. Tengo muchos buenos recuerdos de haber mirado a los gimnastas trabajar y esforzarse para lograr el codiciado 10. Por eso, cuando veo el número 10, pienso en la perfección. Desde entonces, el sistema de calificación de las Olimpíadas ha cambiado y ya no existe más aquél momento cuando los gimnastas podían esperar lograr el 10 perfecto. Aunque el sistema y las reglas de calificación son diferentes actualmente, el deseo de llegar a la perfección persiste. Los gimnastas continúan luchando por la oportunidad de competir en los Juegos Olímpicos y demostrar la "perfección".

En nuestras vidas la perfección es igual de difícil de lograr. Durante los últimos 10 años, el campo del cumplimiento ha cambiado drásticamente: se han implementado reglas y regulaciones que han cambiado completamente el área antilavado de dinero. Pero, igual que los gimnastas olímpicos, los profesionales de cumplimiento también luchan por lograr la perfección. Desde su fundación, ACAMS siempre ha estado allí para brindarle la capacitación y los contactos necesarios para ayudarle a lograr sus objetivos profesionales. Aunque el camino a veces ha sido difícil, ha habido grandes progresos para desbaratar el lavado de dinero y el financiamiento del terrorismo. Este éxito se debe a gente como ustedes que constantemente están trabajando duramente para lograr la perfección en la lucha contra los criminales y sus actividades ilícitas.

El número 10 es el tema principal en esta edición conmemorativa de *ACAMS Today*. El artículo principal *Los 10 mejores consejos de ciber-concientización* ofrece a los profesionales ALD una extensa lista de lo que puede hacerse para ser más efectivo en la mitigación del ciber-riesgo a nivel profesional y personal.

El segundo artículo principal *Retrospectiva: 10 años de ACAMS* es una entrevista profunda con cinco expertos ALD sobre cómo ha evolucionado el campo del cumplimiento, el efecto que ACAMS ha tenido en la profesión del cumplimiento y cómo ha cambiado el escenario del cumplimiento en la última década.

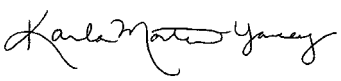
Este año también hace 10 años desde aquél sombrío día del 11/9. Los trágicos eventos que ocurrieron ese año cambiaron las vidas de muchos y dieron nueva forma al campo del cumplimiento. El artículo *11/9… Entonces y Ahora, 10 Años Después* analiza las medidas tomadas desde ese día que pueden haber hecho más seguro al país, y explica las lecciones que hemos aprendido en los últimos diez años en nuestra lucha contra los terroristas y los lavadores de dinero.

Combatiendo al crimen organizado a la antigua: Un estudio de Al Capone es un perfecto ejemplo de cómo las lecciones del pasado todavía pueden ser viables en el complejo mundial criminal actual. Al repasar la investigación de Al Capone desde los años ´20, el autor ofrece una mirada sobre cómo las técnicas utilizadas entonces pueden ser útiles en el mundo actual.

Esta edición incluye muchas entrevistas apasionantes que van desde la entrevista al primer miembro de ACAMS hasta la realizada a su miembro número 11.000. Además, asegúrese de leer *Los 10 primeros del presidente de la junta asesora durante los 10 años de ACAMS*.

Finalmente, tengo el orgullo de anunciar en esta edición el lanzamiento del nuevo sitio en Internet ACAMSToday.org. Este nuevo sitio estará dedicado exclusivamente a brindarles a nuestros lectores ávidos contenido en línea, una interfase web fácil de utilizar y la posibilidad de buscar contenidos anteriores por tema. Asegúrense de visitar www.ACAMSToday.org para leer los últimos artículos sobre el campo del cumplimiento.

A medida que la comunidad ALD sigue luchando para lograr ese 10 perfecto en la lucha contra los criminales del mundo, estoy positiva en que los próximos 10 años traerán un compromiso y éxito constante a la causa en la que todos estamos luchando.



Karla Monterrosa-Yancey, CAMS
editora en jefe

May–July Graduados CAMS

Abdelbasit Abdelathim Mohamed
Robert Abreu
Sarina Accime
Tenaz Aga
Amol Agate
Jalaluddin Ahmed
Raymond Warren Alderton
Iman Kassem Al-Hayafawi
Aftab Ali Khan
Toghrul N. Aliyev
Joao R. Almeida
Meshari Alnusf
Ignacio M. Alvarez
Rosali Andrade
Benny Ang
Luis Aquino
Ron Arcoleo
Ashish Arora
John H. Atkinson
Hugo Antonio Aveda Becerra
Ms. Ayahandayani
Gilbert Ayala
Rana Baasiri
Drew Bach
Scott Badberg
Ana Baiardi
Erin Balabanian
Rosalind Barbour
Lawrence B. Barkerding
Robert Barnett
Florence Barriere
Daniel Bartley
Jerard Basmagy
Manet Basson
Mathew Bastianon
Robert Bates
Kelly Bavaresco
Wassan Bayazid
Dorothy Bearden
Kami Belchak
Julie Benedierks
Giovanni Daniel Benitez Angel
Eduardo Berrizbeitia
Brian Birnie
Robert Bligh
Mario Bogran
Renato Bonuccelli
Manal Bou-Karoum
Marie Boustani
Lesley K. Bove
Tamara Bowen
Elaine Bright
Michael Briskie
Milena Buc
Catalina Calin
Michelle Cao
Stacey R. Carlson
Linda Carmy
Stephanie Howard Carr
Maureen Cassady
Shaun C. Cespedes
Amitabh Chakravarty
Christine Chambers
Cherie Chan
Yat Cheung Chan
Brian Chappell
Clayton Chastain
Amit Chaturvedi
Sergio Jose Chavantes
Rupinder Chawla

GRADUADOS CAMS

Lee Meow Cheng
David D. Chin
Wing Cho
Vijay Kumar Chourasia
Ka Fai Chow
Maria Ciprich
Thomas Clayton
Karen Coates
Tori A. Cohen
John H. Collie
James Connors
George Conrad Bruce
Jorge Contreras
Ronald Cote
Eric Craig
John R. Crouch
Gilbert Dasig
Antonio Davis
Scott Dawson
Gavin D'Cruz
Suelan Melissa De Sormeaux
Melanie Dean
George DeQuattro
Tracy Devine
Royce Dillard
Eugenio DiMira
Joseph Dixon
Maria Dodson
Barbara Donato
Alexander Dumke
David A. Duodu
Myra Duque
Tim Dyball
Antoine Raymond El Hayek
Gillian Elliott
Michelle Emerton
Hugo Escandell
John Evans
Ominu Evbota
José Luis Fajardo Martín
Steve Falvo
Melissa Favorite
Riadh Fayech
Terri Fermo
Aurora Fernandez-Romero
Michael Fitzgerald
Katherine Foster
Dilia Raouf Fouad
Sylvia Freel
Jen Fuller
Laurai Furdui
Blake Gable
Xia Gao
Jimoh I. Garba
Alexandr Garcavenco
Reydom Garcia
Alejandro Gaviria
Marina Gavlovska
Miriana Gjorgjioska
Mauricio Gomez
Estevan Gonzales
Chakradhar Gopichetty Laxman Rao
David Charles Gowan
Jessica Granderson
Russell Grant
Lawrence Stephen Grant-Lapre
Adarsh Gupta
Amit Gupta
Maria Virginia Gutierrez
Rosanna Hampton
Gentry Hardin
Erica L. Harper
Mary Anne Hart
William G. Harvey
Joni K. Hendrix
Yolanda Hilton
Erica Hirsch
Ka Ming Ho
John T. Holland
Doug Holm
Eric Hood
Francis Barchus Hounnonga
Patricia A. Hrubos
Sherry Huber
Sook Young Huh
Amy Hung
Dominic Hurtubise
Abrar Hussain
Afshan Hussain
Jim M. Huvane
Michael Ifill
Joanna Inorowicz
Tanaaz Irani
Hemwattie Itwaru-Gideon
Naomi Iwasaki
Jaquelyn T. Jackson
Thaina Jacques
Juan Carlos Jimenez Diaz
Michael Johnson
Kenneth Jones
Veena Joshi
Thomas W. Jurmanovich
Robert W. Kaiser
Douglas Kamin
Ganesh Kanse
Ahmed Sabry Kassem
Kenji Kasubuchi
Aya Kawai
Beatriz Keeney
Brian Keicher
Miles Kelly
Uzma Khalid
Arifatul Khorida
Karlijn Koel
Drew Kohan
Karolina Koziol
Michelle Marie Kulzer
Ashish Kumar
Chinnaswamy Kumar
George Kunkel
Macrina Labitigan
Nadeen Lahham
Lisa Lai
Jeffrey Lally
Gai Lambourne
Beatriz Lanata
Tracy Landsem
Tanesha J. Larkin
Eva Rosdiana Lase
Boon Kin Lau
Vicki Lau
Gary Leavitt
Kwok Ho Lee
Latena Lee
Wing Shuen Kathy Lee
John Steven Leiter
Ana María Lemmi
Linda Lentz-Senanayake
Abraham Leon
Susanny Leonardi
Renata Lewandowska
Sherron A. Lewis
Jing Li
Benjamin Liceaga Muñoz
Shih-Min Lin
Amy Lindner
Cheri A. Lineberger
Kendrick Lo
Tania Long
Michael P. Looney
Thomas Lorenz
Qiang Lu
Robert Ludwig
Bradley Luker
Ali Lukungu
Rodney MacInnes
David Mackey
Daniel Maclennan
Laura R. Madison
Minerva Magnaye
Sonali Majumdar
Julie Makielski
Jake G. Malasig
Pablo Maldonado
Mark Malinowski
Abdullah Mamun
Helen Man
Vijayalaxmi Manelkar
Stephen Mariotti
Heather Marshall
Grisel Martinez
Carlos Martínez Amial
Jo Ann Masiello
Scott Mauro
Lynda Mayoyo
Jordana Mazal
Conall McGonagle
Tracy McBride
Debra McNamee
Sigifredo Mendoza Mancilla
Viswanath Menon
Bryan J. Metzler
Zachary C. Miller
Frederick Milliken
Keith Mitchell
Chioma Mogbo
Mohammed Ghulam Mohammed
Sahar Eid Mohmoud Youssef
Tino R. Mollica
Kelly D. Moore
Angela Morales
Enrique Morris
Collin Moseley
Aaron Osebimeka Mosugu
Imad Mouaid
Mahasen Moukadem
Izabela Mroczek
Hilda Mussi
Lucila H. Nakagawa
Gerardo Narvaez
Devaki Nathan
Sherry Neeley
Ola Thuen Neergaard
Tom Nesseth
Andrew Nieves
Oluwasimbo Niyi-Ige
Fungai Nyamahowa
Denis Nyambi
Yoshiharu Oikawa
Peggy O'Reilly
Katherine E. Oser
Dan Lohde Otzen
Renato Aldo Padilla Gutierrez
Nitza Pagan
Margie G. Pagdanganan
Jeena Paik
Ellen Dong Mei Pan
Subbaraman V. Panmanna
Kathleen Pattison
Carroll Patton
Noah A. Payton
Tyler Pederson
Dawn A. Pelmear
Kenneth Pemberton
Norma De La Caridad Penate
Yanelis Perez
Babu Perumal
Christopher Gene Phillips
Jin Ping Pi
Michelle Piwowarski
Gordon Plancon
Henry Pleau
Michal Pochec
Dennis Pope
Jeffrey A. Pottorff
Shyrill Powell
Keenan Press
Richard C. Pringle
Robert Pula
Patricia Quan
Manzur Qureshi
Ryo Ra
Tarun Unni Rajagopal
Craig Ramirez
Jorge Ramos
Rowena Rao
Shellie J. Rayford
Nathan E. Reger
Ann Reilly
Justyna Remiszewska
Danny Reynolds
Ngozi Nkem Richard-Uponi
Christine Rickman
Edwin Rivero
Kenneth Robb
Keith Roberts
Eugenia Rodriguez
Ralph Rogers
Pamela Rojas
Michael Rokos
Gilbert Roland
Derek Roos
Kenneth Rosen
Gary A. Rudolph
Mikolaj Rutkowski
Frank Ryckewaert
Nada Sabra
Tomás Salud Correa
Randhir Singh Sandhu
Roberto Sayavedra
Scott Schabel
Ryan A. Schmitz
Craig Schott
Geoffrey Scott
Lucie Semerdjyan
Devi Septiana
Benoit Serrand
Sonal Shah
Ajia Shaheen
Tatiana Shapira
Aseem Sharma
Anton Shchukin
Hong Sheng
Marina Shilova
Kai Chen Shing
Alison Shipley
Jeremy Shirey
Mutiara Sibarani
Debbie Sinard
Parul Ranvir Singh
Abbie Skupien
Ken Smith
Travis Smoot
Christine Soares
Seeta Sobrian
Sai Rene Soh
ZhiBock Soh
Devanaden Sooprayapatten
Fran V. Sponsler
Pedro Stachera Sobrinoh
Magdalena Stefanska
Michal Stelmaszuk
Kathleen Stenger
Karen Stensgaard
Susan Stevenson
Glen Stover
Phyllis Strand
Richard Jeremiah Struck
Mr. Sudarta
Habib Jibrin Suleiman
Dini Sulliati
Chastity Swantz
Nathalie Szekely
Ellen Szeto
Aik Chin Tan
Denise Taylor
Patricia Tennant
Delphine Teo
Matthew Thatcher
Monique Thenier
Raquel Thompson
Jorge Ricardo Torres
Lucy Tran
Stephen Dat-Yin Tse
Stephen Tseronakis
Amanda Tucker
Umit Turkkan
Williiam Tyack
Heather Tyrrell
Arthur R.C. Van Kampen
Alexandria P. Vanasco
Sylvie VanDijk
Greta Vanzeebroeck
Ellen Veneberg
Jaron Villafana
Regis Vincey
Victor Vizcaino
Dorina Vornicescu
Heather Wahl
Robert Wallace
Robert Ward
Sheela Warrier
Regina Waterhouse
Todd G. Wauls
Hillary Wehrer
Dean Wheeler
Beth Wilde
Pamela Wilkerson
Kenneth Will
Rodney Willis
Michael James Wilson
Albert Wolders
Meredith P. Wong
Maxine Wu
Frank Xu
Jennifer L. Yager
Hiroshi Yamamoto
Joseph Teng Chieh Yang
Wei Yi Li
Rei Ng Yi Yun
Andrew Yonda
Karen A. Youell
Trifaldi Yudistira
Imran Zafar
Nestor Zaragoza
Carina Ying Zhang
Haiying Zhang
Huanhuan Zhang
Vivien Xia Zhao

Sepideh Behram
Gaithersburg, MD, EE.UU.

Sepideh Behram es el vicepresidente de Cumplimiento Global y Ética de Tarjetas Comerciales Globales de American Express. Antes de ingresar a American Express, Behram fue oficial de cumplimiento jefe de Travelex Global Business Payments, Inc. para América del Norte, supervisando todo el cumplimiento regulatorio y las funciones de habilitación de la compañía.

Previo a su ingreso a Travelex, Behram fue asesora senior de cumplimiento en el Centro de la Sección de Cumplimiento Regulatorio de la Asociación de Banqueros de los EE.UU., supervisando los esfuerzos regulatorios sobre el antilavado de dinero y los temas de la Ley de Secreto Bancario, emitiendo cartas con comentarios y haciendo participar a la industria en discusiones sobre la legislación propuesta.

Antes de desempeñarse en ABA, Behram fue Directora Antilavado de Dinero Global de E*TRADE Financial y suboficial de cumplimiento jefe de E*TRADE Bank además de tener varios cargos en el Monroe Bank and Trust en Monroe, Michigan, incluido el cargo de segundo vicepresidente y gerente especial de bienes, supervisando el cumplimiento y cobros de los préstamos comerciales.

Behram obtuvo el título de abogada en la Escuela de Derecho de la Universidad Estatal de Michigan y el grado de Bachiller en Artes en Ciencia Política en la Universidad George Washington. Ella es miembra de los Colegios de Abogados del Distrito de Columbia y de Michigan y de la Asociación de Abogados de los EE.UU. Behram es directora miembra del Capítulo de la Capital de los EE.UU. de ACAMS.

John Schmarkey, CAMS, CFE
Atlanta, Georgia, EE.UU.

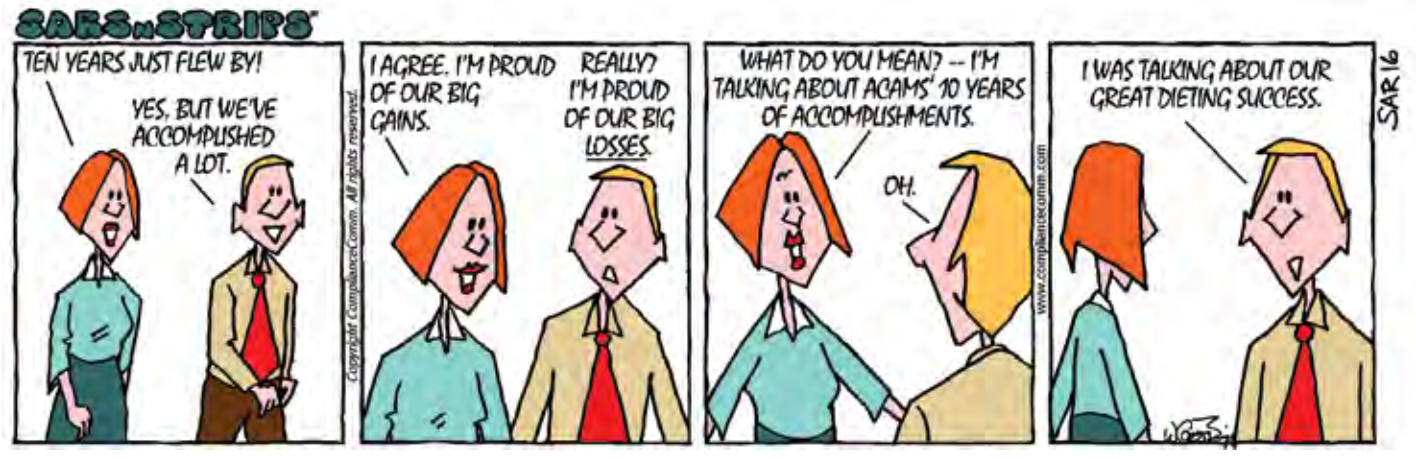
John Schmarkey es un miembro CAMS y un activo Examinador de Fraude Certificado, que ha trabajado en Investigaciones Criminales del Servicio de Rentas Internas del Departamento del Tesoro de los EE.UU. durante veintisiete años como agentes especial senior. Tiene una amplia experiencia en investigaciones de fraude impositivo y fraude financiero y temas de lavado de dinero con aspectos internacionales. Esto incluye una década actuando en los grupos de trabajo del crimen organizado y de terrorismo, con experiencias de investigaciones en el sudeste asiático, en Europa y en Latinoamérica. También tiene experiencia internacional en la comunidad de inteligencia y como lingüista. Schmarkey tiene experiencia en el sector no gubernamental en contabilidad pública y fabricación. Actualmente es un miembro de la junta, vicepresidente y controlador de una empresa de productos forestales. Es miembro de la Junta Asesora del Centro de Estudios Forenses en Contabilidad y negocios, en la Universidad del Sur ge Georgia. Expone en clases de colegio y grupos profesionales sobre fraude y lavado de dinero. Le gusta interactuar y es entrenador de equipo en el Proyecto Adrian, en seminarios de investigaciones de fraude y el a elaborado y presentado cursos en el Centro Federal de Capacitación en Control Legal.

Paulina M. Zurowska, CAMS
Chicago, Illinois EE.UU.

Paulina M. Zurowska es una experimentada investigadora profesional que ha estado en la industria bancaria durante diez años y tiene una amplia experiencia en el antilavado de dinero. Actualmente es la oficial antilavado de dinero asistente de control de calidad de BMO Harris Bank N.A. Su role es colaborar en la creación de un programa AML CC (o QA, por sus siglas en inglés) en BMO Harris así también como la realización de revisiones de control de calidad, varios exámenes y reporte de temas y supervisión ALD.

Antes de ingresar a BMO Harris era la jefa de equipo del departamento LSB del Park National Bank (un banco de los EE.UU.), donde su función principal era el control de calidad y la supervisión de las funciones diarias del departamento. Mientras estuvo allí, Zurowska ascendió desde su rol inicial como analista LSB (dedicada especialmente al monitoreo e investigaciones de actividades sospechosas) lo cual le brindó una atención única y detallada del enfoque en las investigaciones. Antes de ingresar a Park en septiembre de 2007, Zurowska trabajó en el MidAmerica Bank (PNC) desde 2002 y ocupó varios cargos en el área minorista. En 2006, Zurowska fue promovida al Departamento de Prevención de Pérdidas como analista y finalmente comenzó su carrera en el antilavado de dinero en 2007.

Zurowska se graduó en 2005 en la Universidad de Illinois en Chicago con el título de Bachiller en Artes Liberales y Ciencias, con especialización en Justicia Criminal. Ella es Especialista Certificada en Antilavado de Dinero desde 2008. Zurowska también es miembra de la junta ejecutiva del Capítulo de Chicago de ACAMS. Ha sido codirectora de membresía del capítulo desde marzo de 2010. Tienen una activa participación en la membresía del capítulo y en la conservación y ampliación de la cantidad de miembros del capítulo.



Producido por ComplianceComm

10 Años y Seguimos Contando

¡Gracias a la Comunidad de ACAMS!

Constantemente escucho a la gente lamentarse por lo rápido que pasa el tiempo, y con demasiada frecuencia todos descuidamos reflexionar adecuadamente sobre el progreso. Bien, a medida que nos acercamos al décimo aniversario de ACAMS, el personal de ACAMS y yo ciertamente queremos agradecer a los ahora más de 11.000 miembros por hacer que nuestra organización sea el líder global en ALD. Los últimos 10 años nos han desafiado a todos nosotros pero la comunidad ALD ha trabajado diligentemente, tanto en el sector privado como en el público, en una campaña conjunta contra el financiamiento del terrorismo, los carteles de la droga, los criminales de cuello blanco y varias formas de corrupción. Los miembros de ACAMS nos han aconsejado y asesorado sobre una gran variedad de temas, y seguimos contando con ustedes. Sea que hayan tenido cargos en nuestra Junta Asesora, Capítulos o Grupos de Trabajo, hayan sido entrenadores en nuestros seminarios de preparación CAMS, se hayan presentado en nuestras conferencias, seminarios o webseminarios; o dado su punto de vista en las páginas de *ACAMS Today*, no podríamos ser efectivos sin ustedes.

Esperamos ansiosamente los próximos 10 años con el mismo entusiasmo y expectativa.

Una Década de Obligaciones En Expansión

Uno de los mayores desafíos de ACAMS ha sido asegurar el mantenernos actualizados y competentes ante nuestros desafíos. Un oficial ALD en 2011 necesita saber, o al menos estar al tanto de, las leyes, reportes y guías nacionales e internacionales. Los temas actualmente son tan dispares como las sanciones, sobornos, crimen financiero, tráfico de drogas y toda una variedad de fraudes. Los organismos regulatorios cada vez más temen no detectar violaciones de cumplimiento, por lo que las críticas formales son cada vez mayores. La respuesta global a las crisis económicas (en 2008 y ahora) ha agregado nuevas e importantes obligaciones no vinculadas con ALD que seguramente impactarán en las decisiones sobre los recursos. Finalmente, la creatividad de los lavadores de dinero no conoce fronteras, por lo que los nuevos productos se vuelven vulnerables al uso ilegal.

Todos estos cambios tienen un enorme peso sobre la comunidad ALD por lo que las herramientas mejoradas y flexibles son muy solicitadas.

ACAMS ampliará sus ofertas para ayudarles a mantenerse por encima de estos cambios.

ACAMS Responde

Este año, temas específicos como el tráfico humano, han sido populares entre nuestros miembros que están ávidos de obtener la mayor cantidad de información que sea posible sobre cómo ocuparse de este horrible crimen. Nuestro webseminario y la página web sobre el tema han reunido a cerca de 5.000 participantes. ACAMS también encabezó la creación del Grupo de Trabajo sobre Tráfico Humano, copresidido por miembros que representan a los sectores privado y público.

Reconocemos el enorme valor de la comunidad de control legal con ACAMS y dedicamos toda la edición de Marzo-Mayo 2011 de *ACAMS Today* a aquellos heroicos hombres y mujeres. También iniciamos reuniones de intercambio de información que alertaban a ambos sectores sobre los riesgos emergentes y las respuestas posibles.

La importancia de las auditorías ALD nos llevó a ofrecer un webseminario muy exitoso (más de 7.000 participantes) trabajando en conjunto con varias organizaciones internacionales de auditoría. ACAMS, al momento de escribir esta columna, también está trabajando para la creación de capacitación avanzada y credenciales para aquellos en la comunidad de auditoria ALD, la primera de muchas de esas expansivas ofertas.

El reconocimiento a las varias industrias, además de la banca tradicional, que necesitan conocimientos ALD ha llevado a ACAMS a ofrecer programas relevantes y crear grupos de trabajo para los negocios de valores, seguros y negocios de servicios monetarios. Además, tenemos planeado revisar o crear grupos de trabajo sobre sanciones,

tecnología y unidades de inteligencia financiera. Visiten el sitio www.acams.org para obtener más información sobre estos grupos y envíennos sus ideas para otros grupos de trabajo adicionales.

El crecimiento de los capítulos de ACAMS también ha sido un importante objetivo de la organización, y en el último año ha podido hacer que más miembros participen y se unan a los capítulos de ACAMS. Hemos aumentado la cantidad de capítulos, y pasamos de seis en 2009 a 17, y, estamos a mediados de 2011 y seguimos aumentando. Los capítulos difunden la información sobre ACAMS y son vehículos para mejorar las oportunidades de conocimiento entre colegas durante todo el año. Muchas gracias a todos los miembros de los capítulos por su apoyo constante.

ACAMS Today
La última palabra en conocimientos ALD

Finalmente, no podríamos estar más orgullosos de esta publicación, al iniciar los próximos diez años. Karla Monterrosa-Yancey, nuestra Editora en Jefe, ha hecho un trabajo estupendo al identificar a autores, asegurar una diversidad de temas y brindando a la comunidad de ACAMS con la relevancia y oportunidad. A medida que avanzamos para ofrecer una versión en línea de esta publicación, las oportunidades para brindar a los profesionales ALD y otros profesionales los recursos que necesitan para obtener sus conocimientos no tendrán límites.

Juntos, el personal de ACAMS y sus miembros abordarán los próximos diez años con dedicación y compromiso constante.

¡Muchas gracias!

John J. Byrne, CAMS
vicepresidente ejecutivo

Los 10 primeros del presidente de la junta asesora durante los 10 años de ACAMS

Al tiempo que festejamos nuestro décimo aniversario como la única asociación verdaderamente dedicada a reunir a los profesionales ALD de todos los sectores, estoy impresionado por la magnitud de nuestros logros. Hemos creado un foro valioso y colaborativo donde todos tenemos el objetivo común de impedir que elementos malos hagan uso del sector financiero para favorecer sus viles actividades. Tenemos el mejor programa de certificación que es reconocido en todo el mundo. Durante estos 10 años, ACAMS ha crecido en tamaño, talla e influencia. En honor de nuestro décimo aniversario, creía apropiado identificar, desde mi perspectiva, "Mis Mejores 10 Aprendizajes Durante los 10 Años de ACAMS".

10. Un informe del Senado que lo identifica a uno por su nombre nunca es una cosa buena.

9. El "Enfoque Basado en el Riesgo" puede no significar realmente basado en el riesgo.

8. Usted puede conseguir otra cosa que no sea pollo en el almuerzo en una conferencia — puede ser.

7. Siempre deberíamos anticipar que en cuanto todas nuestras políticas y procedimientos estén finalizadas, necesitaremos cambiarlas porque una regulación modifica algunas palabras, p.e. "valor acumulado" por " acceso prepagado".

6. Si bien trabajar para el gobierno está bueno, trabajar en el sector privado es igual de gratificante.

5. Proponer una regulación de "Conozca a Su Cliente" y ser castigado por toda una industria no necesariamente arruina su carrera.

4. ¡Hacer que los Oficiales de Cumplimiento Antilavado de Dinero vengan a Las Vegas no es algo malo!

3. El PIC parecía tan simple — ¡¡¿¿qué pasó??!!

2. No importa lo que digan, no existe eso que llaman "lavado de dinero en reversa" y no debería encargársele a las instituciones financieras la tarea de encontrar terroristas, sino alentarlas a identificar vigorosamente las actividades sospechosas que el gobierno pueda vincular con terroristas conocidos.

1. Los Oficiales de Cumplimiento Antilavado de Dinero son una raza especial de individuos altamente motivados, que trabajan arduamente dedicados al objetivo común de desbaratar a "los malos!". A

Rick Small, CAMS, Presidente de la junta asesora de ACAMS, vicepresidente, Enterprise Anti-Money Laundering, Anti-Corruption, Sanctions, American Express, Nueva York, NY, EE.UU., rick.small@aexp.com

NICE · ACTIMIZE

www.actimize.com

Overwhelmed by regulatory requirements & resource constraints?

Know Your Customer (KYC) • Ongoing Customer Due Diligence • Sanctions/Watch List Screening • Transaction Monitoring

In response to heightened regulatory scrutiny, financial institutions are challenged to address compliance obligations while efficiently managing available resources and long-term costs. NICE Actimize has a deep understanding of these challenges and is helping leading firms across the globe – including retail and investment banks, brokerages, and insurance providers – meet ongoing compliance needs with a comprehensive suite of AML solutions.

Address your firm's compliance needs with Actimize's integrated suite of AML solutions. By providing organizations the ability to share information across the enterprise, Actimize enables streamlined detection, investigation, and management of potential AML risks, while providing the flexibility needed to quickly adapt to changing regulatory and business requirements.

Association of Certified Anti-Money Laundering Specialists® ACAMS®

Platinum Affiliate Member

Leaders in Innovation
MOST INNOVATIVE
ANTI-MONEY LAUNDERING
SOLUTION PROVIDER
www.financial-i.com

i Award Winner 2010

Operational Risk & Regulation 1st compliance software rankings

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

Tokyo:
813 5408 9050

Francisco Monteagudo: El primer miembro de ACAMS

ACAMS Today se reunió con nuestro primer miembro, Francisco Monteagudo, para un rápido viaje al pasado y un repaso actual de cómo ha cambiado el campo del cumplimiento en los últimos diez años.

Monteagudo es gerente de auditoría senior de Jon Campbell Associates Inc. en Brandon, estado de la Florida, EE.UU. Sus responsabilidades incluyen la realización de auditorías de cumplimiento regulatorio de bancos pequeños y medianos. También participa en proyectos especiales, como la revisión histórica de las operaciones en las cuentas de los clientes para detectar operaciones sospechosas, y la realización de sesiones de capacitación en cumplimiento.

Antes de ingresar a Campbell and Associates, Monteagudo fue vicepresidente senior de cumplimiento de Pinebank, N.A., director de control interno y de cumplimiento de American Express Bank International, vicepresidente/cumplimiento y oficial CRA de Home Savings Bank FSB.

Monteagudo también es Examinador de Fraude Certificado, Gerente de Cumplimiento Regulatorio Certificado, Auditor de Servicios Financieros Certificado y Auditor Bancario Certificado.

ACAMS Today: ¿Cómo se enteró por primera vez de ACAMS y qué lo llevó a unirse a la asociación?

Francisco Monteagudo: Me enteré por primera vez sobre ACAMS cuando recibí el paquete inicial en el correo anunciando la creación de la organización. Pensé que había llegado el momento para que los Oficiales LSB/ALD tuvieran su propia organización que estuviera equipada específicamente para los temas LSB y ALD. Envié mi solicitud de membresía a los pocos minutos de haber recibido el paquete.

AT: ¿Supo que era la primera persona en ingresar a ACAMS?

FM: Mi certificado de membresía no tiene un número en el texto, por lo cual no supe que había sido el primer miembro hasta 2004. Tim Heine, asesor legal general de American Express (para quien trabajaba en ese momento) lo anunció en la conferencia ALD.

AT: ¿Cuándo empezó a trabajar en el campo del cumplimiento?

FM: Empecé a trabajar por primera vez en el campo del cumplimiento cuando era auditor en American Savings en Miami a mediados, fines de la década del '80. El Departamento de Auditoría realizaba auditorías LSB y de cumplimiento de préstamos. La auditoría LSB consistía en ese momento de la revisión de los RTEs solamente, ya que no había otros requisitos en esa época. Las auditorías de cumplimiento de préstamos implicaba la revisión de las obligaciones de Veracidad en los Préstamos *(Truth in Lending)* (Reg. Z) y los requisitos RESPA. Virtualmente no había obligaciones de cumplimiento en los depósitos en ese momento ya que las regulaciones de Verdad en los Ahorros *(Truth in Savings)* (Reg. DD) y de tenencias de cheques (Reg. CC) entraron en vigencia más tarde.

AT: ¿Cómo ha cambiado el campo del cumplimiento en los últimos diez años?

FM: Hemos visto el advenimiento del verdadero profesional de cumplimiento. Debido a la gran cantidad y complejidad de las obligaciones de cumplimiento, los profesionales de cumplimiento ahora deben estar muy capacitados, ser muy experimentados y ser miembros de la gerencia superior. Los días en que se le asignaban las responsabilidades de cumplimiento a un empleado porque no había otro lugar para ellas en la organización se han terminado.

AT: ¿Cómo le ayudó ACAMS en su carrera?

FM: ACAMS me ayudó manteniéndome al tanto de las tendencias actuales en el mundo LSB/ALD. No importa lo experimentado que uno pueda ser, es difícil estar actualizado sobre todos los temas a nivel global, y ACAMS definitivamente me ayuda a mantenerme informado y actualizado.

AT: Como auditor de cumplimiento, ¿cuáles son las principales debilidades que ve constantemente en los programas de cumplimiento?

FM: El trabajar para Campbell and Associates durante los últimos cinco años, me da la posibilidad de ver los trabajos internos de muchos bancos en todo el estado. Hay un denominador común para los bancos que tienen programas de cumplimiento exitosos y eso es el compromiso. Los oficiales de cumplimiento tienen que estar comprometidos con sus asociaciones de cumplimiento locales (como ACAMS y otras asociaciones de cumplimiento), con sus reguladores, la gerencia superior, y con todos los aspectos de sus organizaciones. Ése es un factor importante para estar al corriente de todos los cambios y las expectativas regulatorias. Asegura que todos estén en sintonía. Además, el Oficial LSB debe ser un miembro de la gerencia superior. Ellos deben ser capaces de tomar decisiones de alto nivel e incluso de dejar de lado decisiones gerencias cuando crean que corresponda.

AT: ACAMS está evaluando activamente agregar una certificación avanzada para los auditores ALD. ¿Cómo mejoraría eso los conocimientos de la comunidad ALD?

FM: A medida que pasó el tiempo, los temas, los problemas y los programas ALD se han vuelto más complejos. Los Oficiales LSB deben seguir anticipándose a las situaciones estando al tanto de las tendencias y prácticas que pueden no impactar en su organización en el momento, pero que podría hacerlo en el futuro. Una certificación avanzada ALD definitivamente ayudaría en este aspecto.

AT: ¿Cuál es el mejor consejo que recibió durante su carrera de cumplimiento?

FM: Ser preactivo, no reactivo. Anticiparse a la situación estando al tanto de los cambios regulatorios que se aplican desde hoy y no cuando se aproxima la fecha de implementación. Uno dormirá mejor.

Entrevistado por Karla Monterrosa-Yancey, CAMS, editora en jefe, ACAMS, Miami, FL, EE.UU, editor@acams.org

¡Felicitaciones a Hamish MacKenzie, nuestro miembro número 11.000!

Hamish MacKenzie es gerente del grupo de Auditoría Interna y Riesgo de SKYCITY Entertainment Group. SKYCITY es una importante empresa de entretenimientos y juegos de apuestas de Nueva Zelanda (en Auckland, Hamilton y Queenstown) y Australia (Adelaide y Darwin).

Las responsabilidades de MacKenzie en SKYCITY incluyen: Asegurar que el programa de auditoría interna anual de SKYCITY sea cumplido de acuerdo con los estándares globales de mejores prácticas; la entrega de información precisa, objetiva, oportuna e independiente de operaciones clave, riesgos y controles financieros y gerenciales, supervisión del programa de seguros de SKYCITY y reclamos por responsabilidad pública, y la revisión comercial de los contratos más importantes.

Previamente, MacKenzie fue el jefe de seguro de riesgo y auditoria del minorista líder de Nueva Zelandia, Farmers, y antes fue director asociado del equipo de auditoría interna y servicios de asesoramiento de riesgo de KPMG.

MacKenzie es además Contador Colegiado y miembro de la IIA e ISACA. Fue miembro de la junta del Instituto de Auditores Internos de Nueva Zelandia y fue el primero en recibir el premio "Auditor Interno del Año" del Instituto de Auditores Internos de Nueva Zelandia.

ACAMS Today tuvo la oportunidad de conversar con nuestro miembro número 11.000 de Nueva Zelanda en oportunidad del décimo aniversario de ACAMS.

ACAMS Today: ¿Cómo empezó a actuar por primera vez en el campo del cumplimiento?

Hamish MacKenzie: Inicié mi carrera profesional como contador graduado en una firma Contable Colegiada mediana en Nueva Zelandia.

La ventaja de adquirir experiencia con una firma mediana fue que obtuve una capacitación fabulosa en numerosas disciplinas contables fundamentales que incluyeron la auditoría externa, la auditoría interna, la administración del riesgo, impuestos y sistemas de información.

Esto naturalmente me llevó a ser un especialista en auditoría interna y rol del riesgo en KPMG lo que me permitió continuar dando asesoramiento en cumplimiento y consultoría a una gran variedad de clientes.

AT: ¿Cuándo escuchó por primera vez hablar de ACAMS y qué lo llevó a unirse a la asociación?

HM: Me enteré de ACAMS cuando ingresé a SKYCITY. En ese momento, nuestras operaciones de Casino Australiano estaban incluyendo programas ALD/CFT luego de la promulgación de la Ley Australiana ALD/CFT en 2006.

Desde entonces creo que ACAMS es una buena fuente de información y guía para los temas vinculados al ALD y decidí ingresar a ACAMS para aprovechar las oportunidades de contacto con colegas locales, las presentaciones y eventos organizados por el capítulo de Australia-Asia de ACAMS.

AT: ¿Cuál considera que es el mayor desafío para los profesionales de cumplimiento en Nueva Zelanda?

HM: Nueva Zelanda ha anunciado recientemente modificaciones a las regulaciones ALD/CFT.

Si bien Nueva Zelanda había tenido anteriormente varias obligaciones ALD/CFT, estas nuevas regulaciones incluirán varias obligaciones nuevas que requerirán un trabajo importante y los esfuerzos combinados de los profesionales de cumplimiento, los negocios y nuestros reguladores para cumplir con el plazo de implementación del 30 de junio de 2013.

AT: ¿Qué clase de capacitación considera que sería la más ventajosa para los profesionales de cumplimiento en 2011?

HM: Creo que todos los profesionales de cumplimiento, sin importar si son oficiales de cumplimiento ALD, auditores internos o gerentes de riesgo, pueden hacer un mejor uso de las herramientas de análisis de información y las de auditoría asistida con computadora (CATTs, por sus siglas en inglés) para concentrarse en nuestras revisiones.

Entrevistado por Karla Monterrosa-Yancey, CAMS, editora en jefe, ACAMS, Miami, FL, EE.UU., editor@acams.org

Retrospectiva: 10 años de ACAMS

ACAMS Today reunió a los panelistas de la primera sesión de este año para una charla reflexiva sobre los últimos 10 años de ACAMS y el área del cumplimiento.

John Byrne, Al Gillum, Mike McDonald, Saskia Rietbroek y Dan Soto estuvieron presentes en la primera conferencia de ACAMS en 2002. Todos los panelistas compartieron sus recuerdos de ACAMS durante esta década pasada y sobre cómo ha evolucionado el campo del cumplimiento.

ACAMS Today: ¿Cuándo tuvieron conocimiento por primera vez acerca de ACAMS?

Mike McDonald: Yo participé en las primeras etapas del desarrollo de ACAMS y supe acerca de ACAMS al mismo tiempo que Saskia, cuando finalmente decidimos el nombre de la asociación.

Saskia Rietbroek: En el proceso de idas y vueltas de algunos planes estratégicos de Alert Global Media, la idea de una asociación de profesionales ALD nació a mediados de 2001, un par de meses antes del 11/9. Yo asistí a la Conferencia Anual de la Asociación Estadounidense de Ejecutivos de Asociaciones en agosto de 2011, para aprender qué eran las asociaciones. También envié una encuesta por correo electrónico pidiéndole a la gente que votara el nombre de la asociación y también el nombre de la credencial. Hubo muchos nombres en la encuesta y una de las opciones fue CAML.

John Byrne: Tuvimos que rechazar el acrónimo "CAML" por las calificaciones CAMEL en el sector financiero, creíamos que el nombre de la nueva asociación sería confuso para aquellos en la industria bancaria.

Mike McDonald: La forma en que esta organización empezó se remonta a 1999 y 2000. Mucha gente comenzó a surgir como expertos en el campo del cumplimiento. Los bancos estaban siendo perjudicados porque estaban incorporando a estos denominados expertos que realmente no conocían las leyes y que no eran expertos antilavado de dinero. Así es que surgió la idea de crear una organización que entrenara a los expertos antilavado de dinero. De esta manera, cuando los bancos quieren encontrar un especialista ALD, la credencial CAMS es una indicación de que la persona conoce las leyes y regulaciones ALD.

SR: Otra decisión importante que se tomó al comienzo fue no permitir que nadie fuera protegido para obtener la designación CAMS.

JB: El no proteger a nadie para ello es lo que le ha dado y mantenido la credibilidad y calidad de la designación.

SR: Aún los expertos reconocidos en el campo estaban obligados a dar el examen CAMS para recibir la designación. Nadie absolutamente estuvo protegido en el programa.

MM: Otra decisión importante y exitosa que se tomó al comienzo fue si ACAMS debería o no ser una organización centralizada en los EE.UU. o si ACAMS implementaría los estándares internacionales. La decisión final fue implementar los estándares internacionales y hacer que la asociación fuera una organización internacional.

SR: Al comienzo la mayoría de los miembros de ACAMS eran de los EE.UU., pero el cumplimiento es un tema global y si uno solo conoce acerca de la LSB, a la larga eso no es suficiente. El cumplimiento es y seguirá siendo un tema global.

Al Gillum: Recuerdo en un cocktail después de una de las conferencias de cumplimiento más importantes, donde discutíamos acerca de la charla de la gente que decía que eran expertos en el campo y Charlie Intriago planteó que debía aplicarse un proceso al cual hay que adherir a fin de ser llamado experto en el campo del cumplimiento. Y así, nació el origen de la asociación ACAMS.

Dan Soto: Mi primera exposición a ACAMS fue cuando el fundador, Charlie Intriago, me llamó y me preguntó si quería ser el presidente de la junta asesora de la organización. Por

John J. Byrne, CAMS
Vicepresidente Ejecutivo
Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS)

John se unió a ACAMS como vicepresidente ejecutivo en 2010. John es un abogado regulatorio y legislativo reconocido internacionalmente, con más de 25 años de experiencia en temas de servicios financieros, con conocimientos de supervisión regulatoria, política y administración, antilavado de dinero, privacidad y cumplimientos con el consumidor. Fue el ejecutivo de relaciones regulatorias globales del Bank of America y director del Centro para el Cumplimiento Regulatorio de la Asociación de Banqueros Estadounidenses (ABA, por sus siglas en inglés). John ha recibido numerosos premios, incluida la Medalla al Servicio Excepcional del Director de la Red de Control de Crímenes Financieros del Departamento del Tesoro de los EE.UU. (FinCEN, por sus siglas en inglés) y el Premio al Servicio Distinguido de la ABA por su trabajo profesional en el campo del cumplimiento.

Al Gillum, CAMS
Inspector Postal (Ret.),
Presidente/Fundador
Advanced Compliance Technologies

Mientras ejercía como inspector asistente a cargo en la ciudad de Nueva York, Al inició el desarrollo de un sistema de rastreo automático para detectar el uso de órdenes de giro postal en las actividades de lavado de dinero. Poco después, Al fue asignado a la Oficina Central del Servicio de Inspección como oficial de enlace antilavado de dinero, donde trabajó estrechamente con otras agencias federales de control legal, incluida la DEA, el FBI, el Servicio de Aduanas de los EE.UU., y el IRS, para coordinar importantes investigaciones de lavado de dinero. Al también trabajó con el Departamento de Justicia para ayudar a elaborar estrategias nacionales antilavado de dinero.

Desde su retiro del Servicio de Inspección, Al continúa colaborando con la oficina de cumplimiento LSB del Servicio Postal como consultor antilavado de dinero y analista de sistemas. Él redacta requisitos técnicos para el constante desarrollo del sistema de cumplimiento general LSB y el programa antilavado de dinero del Servicio Postal. Continúa participando en varios seminarios y sesiones de capacitación antilavado de dinero.

Michael McDonald, CAMS
Presidente
Michael McDonald & Associates

Michael es un veterano con 27 años de experiencia en la División de Investigaciones Criminales del Servicio de Rentas Internas (IRS, por sus siglas en inglés). Se retiró en 1998 y fundó una consultora con sede en Miami, especializada en lavado de dinero internacional, Ley de Secreto Bancario, Ley Patriot, decomiso de bienes, cumplimiento y temas relacionados. La firma es una red de agentes especiales retirados, cada uno de ellos con amplia experiencia en investigaciones de lavado de dinero. Durante su desempeño en la División de Investigaciones Criminales del IRS, Mike tuvo varios cargos de agente de campo y de dirección y dirigió a personal de investigación en muchos grupos de trabajo sobre lavado de dinero de alto perfil. Fue el principal director en la creación del primer grupo de trabajo sobre lavado de dinero, la Operación Dólar (Operation Greenback). Fue el primer coordinador del IRS en el Grupo de Trabajo de Control de Narcóticos del Crimen Organizado de la Florida/Caribe y del Grupo de Trabajo del Área de Alta Densidad de Tráfico de Drogas del Sur de la Florida (HIDTA, por sus siglas en inglés). Fue reconocido ampliamente como uno de los principales expertos gubernamentales en los temas de lavado de dinero y la Ley de Secreto Bancario.

Saskia Rietbroek, CAMS, MBA
Socia
AML Services International

Saskia es presidente de AML Services International, y www.nomoneylaundering.com, una empresa que brinda capacitación multimedia constante para el profesional de cumplimiento ALD. Sus webseminarios y eventos de e-aprendizaje mensuales atrajeron a cientos de instituciones financieras de todo el mundo. También realiza auditorías ALD y OFAC, y presta servicios de consultoría ALD/OFAC. Antes de trabajar en AML Services International, ella inició la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS) como su directora ejecutiva fundadora desde septiembre de 2001 hasta diciembre de 2005. Bajo su liderazgo, ACAMS creció en la cantidad de sus miembros desde 0 hasta llegar a los 3500 integrantes de 101 países, y desarrolló el Programa de Especialistas Certificados en Antilavado de Dinero (CAMS, por sus siglas en inglés), que se convirtió de hecho en la credencial antilavado de dinero en la industria de servicios financieros en todo el mundo. Es holandesa de nacimiento, tiene el título de abogada en Holanda y Perú y un MBA de la Florida International. Ha participado en la junta asesora de ACAMS, y actualmente integra el Grupo de Trabajo de Certificación ACAMS.

Daniel D. Soto, CAMS
Oficial de Cumplimiento Jefe
Ally Financial

Dan es el oficial de cumplimiento jefe de Ally, donde es responsable de las actividades de cumplimiento a nivel general de la empresa. Antes de ingresar a Ally, Dan trabajó dos años en el Wachovia/Wells Fargo en las áreas de cumplimiento antilavado de dinero y de banca minorista; durante tres años fue oficial de cumplimiento jefe del Royal Bank of Canada–Centura; y trabajó ocho años en el Bank of America en la función de cumplimiento antilavado de dinero global. Antes de ingresar a la industria privada, Dan actuó en el sector público como examinador bancario comisionado, donde trabajó seis años en la FDIC y casi 10 años con la Junta de la Reserva Federal. Dan vive en Charlotte, Carolina del Norte; es profesor miembro de la Escuela Nacional de Cumplimiento de la Asociación de Banqueros Estadounidenses, e integra las juntas asesoras de la Asociación de Especialistas Certificados en Antilavado de Dinero y la Coalición LSB.

supuesto le dije que le iba a contestar, y llamé a mis colegas Byrne y Small y les pregunté qué pensaban de ello, y por supuesto ellos ya formaban parte de todo esto.

Fue muy importante que el examen tuviera su propio programa y fuera psicométricamente firme, haciendo que de esta manera fuera una organización creíble.

AG: El proceso de escritura del examen ha sido una de las tareas más desafiantes en las que formé parte. Nos costó mucho esfuerzo asegurarnos que fuera un proceso viable aplicado para que el examen pudiera sostenerse ante cualquier comité que deseara auditor el proceso.

AT: ¿Qué recuerdan de la primera conferencia de ACAMS y cómo han cambiado las conferencias con el curso de los años?

AG: Lo que más me llamó la atención de la primera conferencia fue la cantidad de gente que concurrió, a pesar de que la organización estaba en su etapa inicial. Me impresionó la cantidad de asistentes a la primera conferencia.

SR: En la época en que planificábamos la conferencia, barajábamos ideas acerca de los lugares donde podíamos organizar la conferencia y decidimos hacerla en Las Vegas porque era un muy buen lugar para las conferencias. Al principio dudábamos en hacerla ahí porque creíamos que no iba a concurrir nadie del gobierno.

MM: La primera conferencia fue considerada una reunión, no una conferencia. La reunión fue anunciada como un evento para el diálogo abierto y el contacto con colegas.

SR: El evento incluía una "reunión de negocios" para analizar la dirección estratégica de la asociación con los miembros — y esa parte de la conferencia estuvo abierta solo para los miembros.

MM: Las mesas redondas de la primera reunión fueron más informales que las de hoy en día porque los grupos eran más pequeños, pero las mesas redondas resultaron ser un gran éxito.

JB: Después de ese evento, hubo una discusión sobre qué dirección queríamos tomar. ¿Queríamos ser una conferencia, una reunión, un híbrido? Decidimos que debería ser una conferencia pero mantendríamos las mesas redondas y el intercambio de información que es casi tan importante para los profesionales ALD como cualquier sesión general — por lo que sabíamos que queríamos conservar eso. Esto nos distinguirá de otros programas y esto es lo que todavía hacemos hoy. Las mesas redondas continuaron creciendo en popularidad. Una de las cosas importantes que reconocimos desde la primera reunión es que la habilidad para intercambiar información con nuestros colegas es muy importante. Si bien el contenido siempre es importante, la capacidad de conversar sobre temas de interés común distingue realmente al evento de ACAMS virtualmente de cualquier otra cosa en ese momento y también actualmente.

SR: Antes de que se inaugurara ACAMS hicimos muchas investigaciones sobre las asociaciones y descubrimos que había miles de asociaciones, pero no había asociaciones dedicadas a las necesidades e intereses específicos del profesional de cumplimiento.

En la primera reunión en Las Vegas también tuvimos una sesión sobre la carrera profesional donde hubo un asesor en carreras profesionales a disposición de los miembros.

MM: En ese momento no queríamos que esto fuera una conferencia porque no queríamos competir con la conferencia de Moneylaundering.com. Asi que la mantuvimos como una conferencia de trabajo — un híbrido. Los oficiales de cumplimiento reciben más de la conferencia en Las Vegas porque los miembros pueden interactuar con sus pares y analizar los desafíos que enfrentan día a día.

La cantidad de asistentes ha crecido sustancialmente desde la primera reunión/conferencia, pero también ha aumentado la diversidad de los participantes. Uno ahora ve participantes de varias industrias, no solo de la industria bancaria o de control legal. También vemos una cobertura más amplia de participantes tanto geográfica como profesionalmente.

SR: También tuvimos una reunión anual del grupo de trabajo para la primera conferencia. Los miembros del primer grupo de trabajo eran Hussam A. Al-Abed, James Banks, Charles Bates, Jorge Brathwaite, Glady Castellano, Glenn Gottfried, Raymond Gregson, María de L. Jiménez, Domingo Rodríguez y Shirley Webb.

AT: ¿Cuál ha sido el cambio individual más importante en las carreras de cumplimiento en los últimos 10 años?

SR: La gente actualmente necesita saber más que solo lavado de dinero. Antes del 11/9 no había mucha gente que estuviera especializada en el ALD. La mayoría de la gente estaba especializada en el campo más amplio del cumplimiento. Después del 11/9, la carrera de cumplimiento se volvió más especializada y ahora ha completado un ciclo y la profesión de cumplimiento es más amplia nuevamente porque la gente tiene que cumplir muchas funciones debido a la reducción de personal.

MM: Hubo una época en la que los reguladores de todo el espectro eran más agresivos en lo que se refiere a las revisiones del cumplimiento LSB y del programa de cumplimiento ALD de los bancos y los NSMs, en términos de lo que esperaban en las revisiones. Esta agresividad generó un efecto dominó en el comercio y las instituciones no bancarias de todo el mundo.

AG: La única cosa que ha cambiado sustancialmente en la profesión es el sentido de responsabilidad que ahora tiene el oficial de cumplimiento, a diferencia de ocho o diez años atrás, incluida hasta la posibilidad de la responsabilidad personal. El rol o cargo de oficial de cumplimiento ha asumido en los últimos diez años la responsabilidad de mantener a la institución por encima de los reguladores.

DS: Lo que ha sido interesante sobre ACAMS es que los reguladores ahora están preguntando si los oficiales de cumplimiento son CAMS certificados. Cuando iniciamos ACAMS, la idea de que los reguladores buscaran específicamente que esta certificación fuera parte del examen regulatorio no formaba parte de nuestra visión.

MM: Los bancos ahora quieren profesionales de cumplimiento CAMS certificados, lo mismo que los NSMs. La estructura de cumplimiento ha aumentado drásticamente en todas las instituciones financieras.

JB: Dan, tengo una pregunta para ti. ¿Tú crees que es verdad que en la última década se ha dado una mayor prioridad regulatoria al preguntarle a las instituciones? "¿qué tan exhaustivo es el conocimiento de su personal de cumplimiento en el conocimiento del aspecto comercial de la banca?". En otras palabras, con el desarrollo constante de nuevos productos y canales de entrega, ¿no es más importante ahora que digamos 20 años atrás, entender realmente el aspecto del negocio de la institución financiera?. Yo argumentaría que cuando empecé a seguir el tema del cumplimiento muy pocos profesionales de cumplimiento entendían los componentes de la banca. Mientras que ahora si uno no conoce las funciones de su banco van a haber vacíos en su capacidad para realizar supervisión. He visto a algunos reguladores pedir eso específicamente. ¿Has visto eso en alguna institución donde hayas estado?

DS: Absolutamente, si los oficiales de cumplimiento en el desarrollo de nuevos productos no pueden referirse al ALD, ello es considerado como una falla de la institución financiera.

AT: Dejando de lado el 11/9, ¿qué otros eventos en los últimos 10 años han dado forma al panorama del cumplimiento?

MM: La publicación del manual del FFIEC y la publicación del manual de FinCEN para los NSMs fueron muy importantes para la industria. Esto les dio puntos de referencia a las instituciones pequeñas que tenían departamentos de cumplimiento reducidos. Les dio guías para crear y mantener programas ALD más sólidos.

SR: Una cosa más que influyó en el campo es el rol de la tecnología y cómo evolucionó. La cantidad de información que puede encontrarse en Internet ha aumentado significativamente. La tecnología que se usa para detectar actividades sospechosas ha evolucionado enormemente en los últimos seis años. También es más fácil de usar.

MM: La cantidad de compañías tecnológicas se ha disparado desde la primera conferencia.

JB: Otra cosa es la información a la que los profesionales de cumplimiento pueden acceder en línea ahora en 2011. Un banquero en los EE.UU. tiene la misma posibilidad de ver qué está pasado con el GAFI igual que una persona en el Reino Unido. Uno tiene que saber qué hacer con esta información pero esto ha sido un cambio fenomenal no solo para los profesionales de cumplimiento sino para toda la industria.

SR: Uno tiene más información al alcance de la mano para administrar la exposición al riesgo. El cumplimiento ahora es dirigido más a nivel general de la empresa y con un enfoque basado en el riesgo.

AT: ¿Cuál es su recuerdo favorito de ACAMS?

SR: El día en que oficialmente hicimos el lanzamiento de la asociación en la primavera de 2002. Teníamos un stand en la conferencia de Moneylaundering.com y en el primer día tuvimos más de 100 miembros. Eso fue enormemente alentador.

AG: Conocer a gente que tenía responsabilidades y obligaciones similares que las que yo tenía y poder consolarme con mis colegas que entendían totalmente las responsabilidades y dificultades que conlleva estar en el área de cumplimiento. Además, lo que se destacaba era la camaradería y la oportunidad de compartir sus temas de interés con gente en su mismo sector.

MM: Las relaciones que se establecen y la camaradería que se crea a través de la asociación. Hay una credibilidad instantánea cuando uno conoce a alguien por primera vez que es un miembro de ACAMS. Uno tiene una base en común. La mayoría de las relaciones que inicié al principio todavía las conservo. El segundo año de la conferencia anual fue importante porque mostró el crecimiento. El primer año uno no sabía qué esperar. El crecimiento en el segundo año fue más del doble.

DS: Uno de nuestros momentos más brillantes fue la primera vez que organizamos la conferencia anual fuera de los Estados Unidos, en Toronto, fue nuestra declaración de que no iba a ser solamente para los EE.UU. sino una conferencia más del tipo global, igual que lo que éramos nosotros. Reafirmó la declaración de que íbamos a ser una asociación estadounidense.

AT: ¿Qué reservan los próximos 10 años para ACAMS y la profesión de cumplimiento?

JB: Vemos una necesidad real de capacitación avanzada. Estamos en el proceso de armar certificaciones de capacitación avanzada. Vemos que ése es el próximo paso lógico para ACAMS y nuestros miembros. En los próximos años ACAMS también tiene planeado entregar designaciones de conocimiento regional y mantener la naturaleza global de la organización.

AG: Debería enfatizarse el éxito y el crecimiento de la asociación a través de los capítulos locales. La forma en que los capítulos han crecido y evolucionado es sin duda el camino del futuro de la asociación.

JB: La cantidad de capítulo ha aumentado a más del doble en el último año. Este año aún esperamos agregar tres o cuatro capítulos más. Esta es la otra manera en la cual ACAMS ayuda a que la comunidad ALD esté tan conectada — para hablar a alguien que enfrenta los mismos retos que uno y los capítulos son el lugar perfecto para este tipo de intercambio de información. Cada vez que mantenemos una conferencia telefónica en una región donde planeamos inaugurar un capítulo tenemos miembros que nos dicen que ya tienen 30 ó 40 personas interesadas en ingresar al capítulo. Es muy emocionante.

MM: Cuando miro el folleto de la primera conferencia veo que hay siete temas principales que se analizaron en 2002. Los temas principales todavía son importantes en 2011. En los próximos 10 años ACAMS deberá liderar la inclusión de nuevos elementos como la banca móvil y el dinero electrónico.

Entrevista realizada por Karla Monterrosa-Yancey, CAMS, editora en jefe, ACAMS, Miami, FL, EE.UU., editor@acams.org

Fraude y lavado de dinero: ¿Cuál es la conexión?

Los titulares recientes han estado llenos de historias nuevas sobre todo tipo de fraudes, desde el tristemente célebre multimillonario esquema Ponzi de Bernie Madoff, hasta los fraudes de pishing en Internet y el fraude hipotecario. La caída de la economía ha puesto al descubierto a muchos de estos casos, como el fraude hipotecario en los Estados Unidos como resultado del colapso con viviendas.

La gente también habla sobre la conexión que existe entre el lavado de dinero y el fraude. Antes era solo el fraude, pero ahora el lavado de dinero y en un grado limitado también el financiamiento del terrorismo han entrado en escena. ¿Pero, por qué?

El lavado de dinero y el financiamiento del terrorismo reciben más atención porque el LD/FT les permite a los criminales la posibilidad de disfrutar los beneficios de sus delitos. En el caso de los terroristas, les permite disfrutar las escenas de destrucción que generan utilizando el dinero derivado de delitos tales como el fraude para financiar sus actividades terroristas.

¿Cómo se conecta el fraude con el lavado de dinero y el financiamiento del terrorismo? La actividad criminal relacionada con el fraude genera dinero que necesita ser lavado, por lo tanto, donde hay fraude hay lavado de dinero. El fraude es un crimen y es un delito subyacente (estos crímenes son la fuente subyacente del lavado de dinero) de lavado de dinero. En muchas instituciones financieras, existen dos departamentos separados que tratan de proteger a la institución del lavado de dinero y del fraude. En muchos casos, el grupo dedicado al fraude y el grupo dedicado al ALD no se comunican entre sí o no trabajan en conjunto con relación a las amenazas LD/FT que enfrentan en sus respectivos departamentos.

Los departamentos ALD a menudo hacen un trabajo que es similar en naturaleza al del fraude ,pero la razón para hacerlo puede ser muy diferente. Por ejemplo, el sector del ALD trabaja para cumplir con las obligaciones regulatorias ALD, mientras que el sector del fraude trata de proteger a la organización de las pérdidas financieras. Para el sector de fraude es más fácil demostrar el valor del dinero porque al final, puede cuantificar en dólares el impacto de sus esfuerzos antifraude. El sector ALD a menudo es considerado un centro de costos que beneficia al sistema financiero como un todo y a la sociedad en gran medida, pero la organización puede recuperar muy poco para compensar los costos cada vez mayores del cumplimiento.

Las organizaciones pueden beneficiarse conjugando sus recursos de fraude con sus esfuerzos ALD y aprovechando las eficiencias importantes que pueden lograrse mediante una mayor colaboración entre los departamentos de fraude y ALD.

Hace varios años me encontré con un caso que muestra la diferencia entre riesgo de fraude y riesgo de lavado de dinero. Cuando pensamos en el riesgo de fraude, pensamos en el riesgo de pérdida financiera o de pérdida de crédito. La pregunta clave es: ¿está el dinero realmente allí? En lo que respecta al riesgo de lavado de dinero, la pregunta clave es, ¿de dónde vino el dinero? Este caso nos ayudará a entender qué es el riesgo de lavado de dinero comparándolo con el riesgo de fraude.

Detalles de la carpeta analizada del cliente:

- El cliente tiene una cuenta de tarjeta de crédito con un límite de US$2.000, y tiene saldo cero.
- Solo figura una persona en la cuenta de la tarjeta de crédito.
- El cliente realiza un importante pago con cheque por US$20.000 a través de cajero automático.
- Esto crea un saldo de crédito de US$20.000, lo cual es muy inusual para una cuenta de tarjeta de crédito porque normalmente uno le adeuda dinero al banco y no al revés.
- El cliente es un trabajador independiente y trabaja como desarrollador de propiedades y gana US$250.000 anuales.

Ahora, este importante pago con cheque genera un alerta de fraude porque, nuevamente, existe la duda de si ese cheque es válido. Por ejemplo, ¿está el dinero realmente allí? y el banco quiere protegerse contra un cheque fraudulento. El departamento de fraude llama al cliente para averiguar qué sucede. El cliente indica que va a viajar al exterior y quiere utilizar la tarjeta de crédito para obtener anticipos de dinero porque las tarjetas de crédito no son generalmente aceptadas allí. El departamento de fraude considera que esto es razonable y espera a que el cheque ingrese, lo que sucede a los cinco días.

El departamento de fraude no realizó más tareas porque el dinero fue depositado, por lo tanto no hay riesgo de fraude o pérdida para el banco. El departamento de fraude dejó de hacer preguntas y cerró el caso porque nadie preguntó de dónde provino el dinero o si la transacción era razonable para este tipo de cliente de acuerdo con su ocupación, edad o transacciones anteriores.

Mis colegas y yo pensamos que esto era bastante inusual, por lo cual pedimos ver las transacciones de la cuenta del último año y nos sorprendió lo que encontramos.

- Alta velocidad de las transacciones en la cuenta. Había más de 75.000 intentos de transacciones con la tarjeta de crédito en el año y se había aprobado aproximadamente una cuarta parte de las mismas. Si hace las cuentas, no es posible que una persona haga todas estas transacciones.
- Vimos varias transacciones el mismo día a través de distintos canales (teléfono, Internet, en persona), hechas desde distintos lugares, lo que nuevamente sugiere que más de una persona está utilizando la tarjeta de crédito.

- Intentos por hacer extracciones en cajeros automáticos en distintas localidades extranjeras (lugares de mayor riesgo de LD/FT). ¡Los intentos de extracciones fueron realizados incluso después de haberse llegado a los montos máximos, pero siguieron intentándolo!

Por lo tanto la clave aquí es entender que el riesgo de lavado de dinero se refiere a de dónde provino el dinero, mientras que el riesgo de fraude y el riesgo crediticio se refiere a dónde se encuentra realmente el dinero. Los profesionales del fraude ven actividades como esta todo el tiempo, y si hicieran más preguntas, ayudarían a proteger a la organización frente al lavado de dinero y el financiamiento del terrorismo. No cierre el caso considerando que no hay riesgo de pérdida financiera, sino que continúe actuando y pregunte ¿de dónde viene el dinero?

¿Por qué es importante que las organizaciones se protejan frente al LD/FT?

1. Los riesgos reputacional y regulatorio se han vuelto más importantes de administrar en el mundo actual, especialmente con la gran recesión experimentada a nivel global. Este descenso reciente ha hecho que se haya vuelto más crítico para las organizaciones proteger la reputación de la organización de eventos negativos en las noticias. Ningún banco quiere estar en la tapa del diario con un titulo que diga — "El Banco ABC está acusado de lavado de dinero" o el "Banco ABC presta servicios bancarios a terroristas". Esto sería una pesadilla para las relaciones públicas.
2. El cumplimiento con las obligaciones regulatorias relacionadas con el ALD se está convirtiendo en un desafío, ya que el nivel se eleva constantemente. A continuación se detallan los principales organismos o grupos regulatorios que establecen los estándares ALD a nivel nacional y global:

- Oficina del Superintendencia de Instituciones Financieras (OSFI, por sus siglas en inglés) — regulador bancario federal canadiense — ha publicado una guía ALD (B-8).
- Centro de Análisis de Transacciones Financieras y Reportes (FINTRAC, por sus siglas en inglés) — la unidad de inteligencia financiera de Canadá para todas las entidades reportantes, p.e., sector inmobiliario, banca, agentes de valores, negocios de servicios monetarios, contadores, etc. El mandato de FINTRAC es facilitar la detección, prevención e impedir el lavado de dinero, el financiamiento de actividades terroristas y otras amenazas a la seguridad de Canadá.
- Grupo de Acción Financiera Internacional (GAFI) — En respuesta a la creciente preocupación por el lavado de dinero, el GAFI fue creado por la Cumbre del G-7 en París en 1989 para crear una respuesta internacional coordinada. Una de las primeras tareas del GAFI fue elaborar recomendaciones, 40 en total, que establecen las medidas que los gobiernos nacionales deberían tomar para implementar programas antilavado de dinero efectivos.
- Red de Control de Crímenes Financieros (FINCEN, por sus siglas en inglés) — es la UIF de los Estados Unidos y tiene un mandato similar al de FINTRAC. Ha publicado una gran cantidad de material sobre la relación entre el fraude y el lavado de dinero.

3. Los posibles costos sociales y políticos del lavado de dinero, si no se lo verifica o se lo trata de manera efectiva, son serios.
4. El lavado de dinero es una amenaza al buen funcionamiento de un sistema financiero.

Es nuestra responsabilidad colectiva aplicar nuestros mejores esfuerzos para impedir y detectar el lavado de dinero y desbaratar el financiamiento del terrorismo. Aunque puede no haber ahorros de costos directos para la organización, los beneficios que se generan para la sociedad a partir de estos esfuerzos crean un marco y un ámbito para que prosperen las organizaciones legítimas. Los departamentos de fraude y ALD deben trabajar juntos para minimizar estos riesgos.

En el estado actual, la mayoría de las organizaciones tienen departamentos de fraude y ALD separados, pero la tendencia es avanzar hacia una mayor integración debido a la cantidad limitada de recursos y a la economía debilitada. Todos están tratando de hacer más con menos.

Opción Uno: Combinar a los dos grupos en uno

¿Cómo hacerlo?

- Un sistema de monitoreo de transacciones que aplique las reglas tanto sobre fraude como las ALD con alertas generados identificados como resultados de ALD o de fraude.

- Una base de datos concentrada en los clientes que brinde una visión holística de las relación total del cliente con el banco, p.e., todos los productos que tenga, las cuentas en las distintas líneas de negocios, todas las transacciones realizadas por el cliente que sean visibles, etc.
- Un sistema de administración de casos que permita la entrega más fácil de las carpetas entre los analistas y los investigadores.
- El grupo no debería dividirse entre personal de fraude y ALD, sino de acuerdo con las habilidades que tengan sus integrantes. Por ello, en lugar de tener un analista ALD o un analista de fraude que analice las alertas del monitoreo de transacciones, se debería crear un Analista de Delito Financiero (o el título que prefiera), quien sería responsable de la revisión de los alertas ALD y de fraude generados por el sistema de monitoreo de transacciones.
- Un equipo dentro del grupo que estaría a cargo de las tareas de elaboración de políticas y procedimientos, cumpliendo con los cambios regulatorios, comunicándose y trabajando con las líneas de negocios para implementar programas ALD efectivos en los negocios. También tendría a cargo las relaciones con los reguladores y los auditores.
- Designar a un Oficial Antilavado de Dinero que tenga experiencia en temas ALD, no solo en los temas de fraude. Las expectativas regulatorias sobre el Oficial Antilavado de Dinero son muy elevados y se debe cumplir con ello.

Aunque las eficiencias y los ahorros en los costos que se obtendrían de la integración podrían ser importantes, existen serios desafíos relacionados con la integración. Por ejemplo, en la mayoría de las organizaciones el área de fraude está mejor establecida y tiene más recursos que el área ALD, así también como la habilidad para justificar su valor en la organización, mientras que los grupos ALD no pueden cuantificar directamente su valor en la organización y tampoco tienen tanta antigüedad en las estructuras.

Si los dos grupos son fusionados en uno, entonces existe el riesgo de que el ALD pudiera ser absorbido por el sector de fraude y limite los recursos disponibles para el ALD. Esto sería muy peligroso para la capacidad de la organización de mitigar de manera efectiva los riesgos reputacional y regulatorio que enfrenta. Hablando de reguladores, ellos son cautelosos respecto de cualquier reducción de los recursos o el tamaño del sector ALD y esperan que se cumplan todas las obligaciones del Oficial Antilavado de Dinero y del grupo ALD, aún cuando los dos departamentos hayan sido fusionados. Esta opción no es tan simple como unir a dos grupos y pensar que todo va a funcionar porque existen temas muy complejos y también regulatorios que deben ser considerados antes de llevar a cabo cualquier integración.

Opción Dos: Incrementar la Colaboración, no la Integración

Otra opción es mantener separados a los grupos pero formalizar la relación, de manera que los dos grupos trabajen mejor juntos con el objetivo de reducir el riesgo reputacional y regulatorio que enfrente la organización. ¿Cómo se puede lograr esto?

- Haciendo que los grupos reporten al miembro senior del equipo ejecutivo.
- Teniendo un sistema en común de administración de casos para que los casos puedan ser derivados entre los dos grupos.
- Manteniendo sistemas separados de monitoreo de transacciones pero entrenando personal tanto del área de fraude como de ALD para detectar señales de alerta para ambos departamentos. Si el sector ALD está analizando un alerta pero no encuentra nada sospechoso de ALD, podría tratarse de fraude. Entonces ellos debería poder comunicar fácilmente esta información al grupo de fraude para que la puedan analizar más detalladamente. El personal de fraude podría hacer lo mismo si observara alguna actividad que pareciera sospechosa de lavado de dinero o de financiamiento del terrorismo, entonces podría la información al personal ALD.
- Capacitación especializada para departamento sobre varios indicadores del otro departamento.
- El grupo de fraude podría hacer una autoevaluación ALD anual para su área e informar esto al oficial antilavado de dinero.
- El grupo de fraude podría ayudar al grupo ALD entrevistando a clientes para investigar actividades inusuales o sospechosas. Actualmente, el departamento ALD le pide al personal de primera línea que haga esto pero no es tan efectivo porque el personal de primera línea no está entrenado para hacer esto, y existe un elemento de riesgo personal para los empleados.
- Teniendo reuniones regulares entre los dos grupos (como mínimo mensualmente) para analizar estrategias, recibir comentarios para mejorar e intercambiar información sobre los casos.

He conocido varias organizaciones en mis anteriores trabajos donde el departamento de fraude analizaba muchos casos de actividades inusuales pero si no estaban relacionados con fraude, entonces simplemente cerraban el caso. Yo siempre le preguntaba al departamento de fraude cuántas veces enviaron un caso inusual al grupo ALD de todos esos casos inusuales o alertas. ¡La respuesta siempre fue una cifra de un solo dígito! Hay mucho por mejorar si vamos a trabajar juntos para detectar, impedir y desbaratar a los lavadores de dinero, los terroristas y los criminales.

El fraude y el lavado de dinero están intrincadamente conectados tanto en términos de actividad criminal como de obligaciones regulatorias. La pregunta clave al evaluar los riesgos de lavado de dinero y financiamiento del terrorismo que hay que hacer es, ¿de dónde vino el dinero? Mientras que la pregunta clave para evaluar el fraude o el riesgo crediticio es, ¿está realmente el dinero allí? Una vez que conocemos esta importante diferencia, entonces es posible que los departamentos de fraude y ALD trabajen juntos más de cerca para proteger a la organización de los riesgos reputacional, regulatorio y de fraude. El lavado de dinero, el financiamiento del terrorismo y el fraude son todas amenazas para nuestras organizaciones que cada uno de nosotros — sin importar si somos profesionales del fraude o ALD — que necesitamos conocer más y trabajar juntos más estrechamente para vencer. A

Sal Jadavji, CAMS, CFE, oficial ALD jefe, MCAN Mortgage Corporation, Toronto, Ontario, Canadá, salminjadavji@gmail.com

TAMLO™

AML Online Training
for frontline employees

TAMLO International Inc. designs and distributes highly engaging, fully interactive online courses for anti-money laundering and counter-terrorist financing.

TAMLO's **Flag the Money**™ training includes the award winning film, "**Carl's Story**," the compelling account of a wealthy drug-dealing entrepreneur who tries to launder his profits through various sectors, including banks, MSBs, casinos, jewelers and stockbrokers.

Effective

The fictional scenarios and real-life examples show employees how to detect and report activities that might be related to money laundering or terrorist financing.

TAMLO's training courses include a built-in exam that helps to ensure a baseline level of knowledge throughout your organization. Track the results using automatic or customized reports.

Engaging

Students remain engaged throughout the course with interactive exercises, content-rich narration, and interviews with money laundering specialists and counter-terrorism experts.

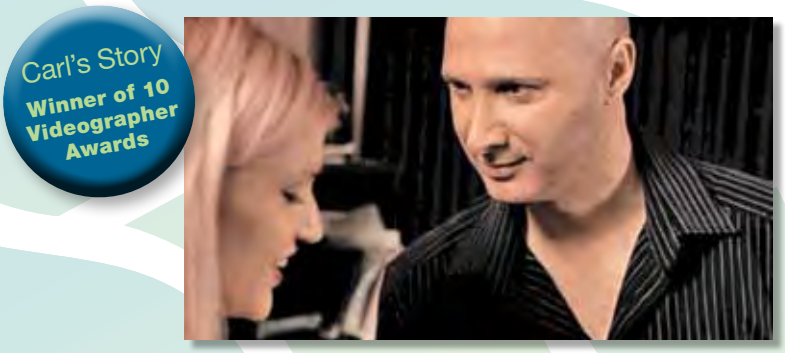
Customizable

The courses are tailored for various regulated sectors and can be customized with:

- your logo and branding
- a video introduction by your spokesperson
- custom content to include your policies and procedures

Access the courses via the internet or install them on your intranet.

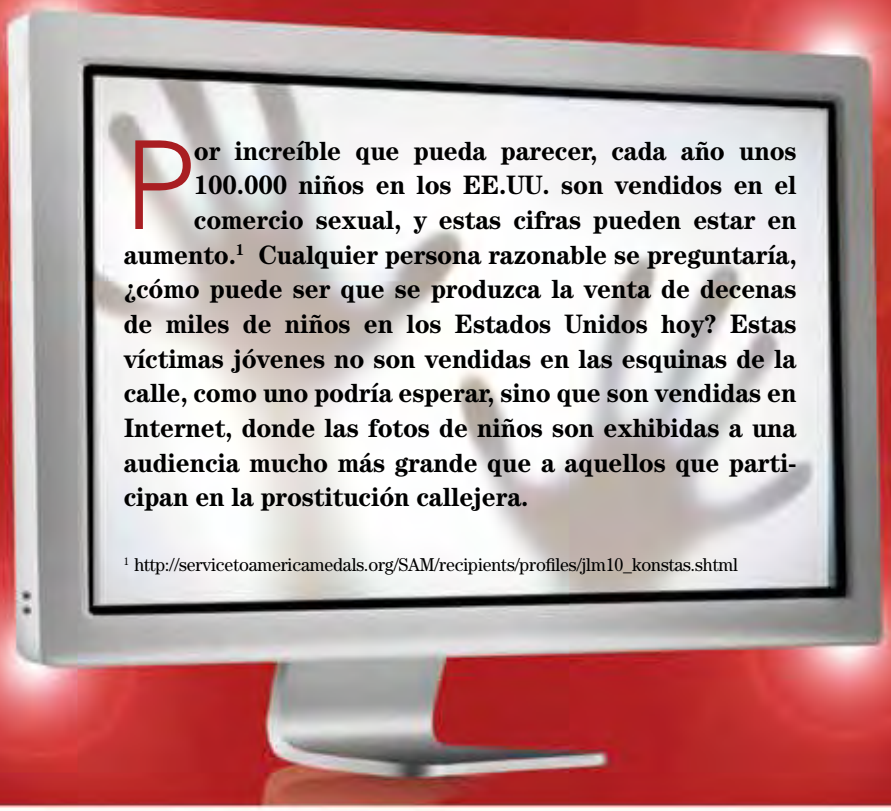
- **Money-back guarantee**
- **Corporate pricing**
- **Volume discounts**



www.TAMLO.com 1-888-998-2650 **info@TAMLO.com** Miami Montreal Calgary

US$5 para arruinar la vida de niños y mujeres:

Anuncios en sitios de Internet utilizados para lavar dinero promoviendo la prostitución/tráfico humano



Por increíble que pueda parecer, cada año unos 100.000 niños en los EE.UU. son vendidos en el comercio sexual, y estas cifras pueden estar en aumento.[1] Cualquier persona razonable se preguntaría, ¿cómo puede ser que se produzca la venta de decenas de miles de niños en los Estados Unidos hoy? Estas víctimas jóvenes no son vendidas en las esquinas de la calle, como uno podría esperar, sino que son vendidas en Internet, donde las fotos de niños son exhibidas a una audiencia mucho más grande que a aquellos que participan en la prostitución callejera.

[1] http://servicetoamericamedals.org/SAM/recipients/profiles/jlm10_konstas.shtml

Los sitios en línea en Internet publican fotos de niños pequeños y adolescentes específicamente con el objeto de vender sus cuerpos por sexo. Sus fotos son observadas por millones de personas en todo el mundo con solo presionar unas pocas veces el mouse de una computadora. Los anuncios en sitios de Internet que publican a niños a la venta no son difíciles de montar. He investigado los pagos en línea de los anuncios en Backpage.com y Craigslist, donde por US$5 a US$10 por anuncio, la gente puede publicar anuncios con fotografías para la venta de sexo. Los proxenetas — vendedores de niños — utilizan los sistemas financieros para aceptar pagos a través de la red de de pagos de Visa y MasterCard, donde tienen la posibilidad de tener una cuenta que les da acceso financiero para pagar la publicación reiterada de anuncios en estos sitios de Internet. Publicaciones recientes de varios fiscales generales de los EE.UU. informan sobre las extensas batallas para hacer que Craigslist cierre su sitio en la red de entretenimientos para adultos en los EE.UU. Finalmente Craigslist cerró el sitio.[2] El mismo pedido se le hizo a Backpage.com; y, hasta hoy Backpage.com se ha negado a cerrar su sección de entretenimientos para adultos donde se publican anuncios de sexo.[3]

Ofrecimientos en línea de prostitución/tráfico humano — un tema en el mundo ALD

Los investigadores ALD harían bien en cambiar los procesos mentales para no limitar más la definición de lavado de dinero que involucre a fondos "ilícitos" resultantes del tráfico de drogas y el financiamiento del

[1] http://servicetoamericamedals.org/SAM/recipients/profiles/jlm10_konstas.shtml
[2] http://www.foxnews.com/scitech/2010/09/04/craigslist-shuts-adult-services-section/
[3] http://news.change.org/stories/backpagecom-refuses-attorneys-generals-requests-to-close-adult-ad-section

terrorismo. Muchos casos de prostitución en línea son en realidad tráfico humano disfrazado. Las "prostitutas" son víctimas del tráfico que están vendiendo sexo involuntariamente. La actividad sexual con un niño es ilegal sea que incluya dinero o no. Cualquier ganancia obtenida de la prostitución en línea, sea voluntaria o no, es "ilícita, ya que la actividad subyacente es ilegal. En el siglo XXI, el tráfico de seres humanos a través de pagos de anuncios que son abonados a través de nuestros sistemas de pago es solo un ejemplo de delitos más tradicionales que utilizan "alta tecnología" y que llegan a una audiencia más amplia. Para existir a gran escala, estos criminales deben tener acceso a Internet así como también a los sistemas de pago que apuntalan también a nuestro comercio legítimo. Los expertos estiman que un 76% de las transacciones por sexo con niñas menores son procesadas a través de anuncios en Internet. La investigación muestra que el costo de un anuncio en los sitios de Internet es tan solo de US$5. Eso puede repetirse — US$5 para publicar la foto de un ser humano a la venta. El bajo costo de ingreso es un factor clave para los perpetradores. La posibilidad de mover la "mercadería" fácil y anónimamente de un sitio a otro simplemente descargando la fotografía hace que el delito sea aún más atractivo para los criminales que no consideran que la vida humana tenga ningún valor.

Reportes de Actividades Sospechosas

Los investigadores ALD saben que el Título 18 U.S.C. § 1956 : Código de los EE.UU. — Sección 1956: Lavado de instrumentos monetarios incluye entre sus "actividades ilegales específicas" en la sección (vii) el tráfico de personas, la venta o compra de niños, la explotación sexual de niños, o el transporte, reclutamiento o esconder a una persona, incluido un niño, para actos sexuales comerciales" es ilegal.[4,5] Así, los criminales que participan en estas publicaciones en línea que generan fondos de esas actividades son susceptibles de ser enjuiciados por lavado de dinero. La identificación de un sitio por su posible utilización para actividades tan atroces, sin embargo, requiere que tengamos un mayor conocimiento de estos sitios, para que podamos presentar mejor los Reportes de Operaciones Sospechosas (ROSs). Los ROSs pueden y deberían ser utilizados para reportar transacciones que puedan estar siendo utilizadas por individuos sospechados de realizar tráfico humano, sea que se trate de esclavitud laboral o de tráfico sexual. Desafortunadamente, el actual formulario del ROS presentado por DI incluye en la lista al fraude, lavado de dinero, actividades terroristas, pero no contiene ningún casillero separado para el tráfico humano.[6] Es hora de que el ROS sea actualizado para que incluya el tráfico humano que pueda ser anunciado a través de sitios en Internet que son pagados a través de nuestros sistemas financieros. Hasta que el formulario no sea actualizado para identificar al tráfico humano como un delito subyacente de lavado de dinero, quienes completen los ROSs pueden continuar utilizando el casillero identificado como "otro"; y asegurar que las palabras claves sean incluidas en la Parte V, Descripción. En cuanto a esto, también, sería útil trabajar con frases clave que podrían ser incluidas en la descripción que las autoridades de control legal podrían identificar con términos clave en el análisis de los términos incluidos en los ROSs, y otros que podrían apuntar al tráfico de niños. Otra recomendación es que FinCEN publique un alerta con textos sugeridos como "Descripción" para los DIs, los NSMs y otros a ser utilizados en la presentación de ROSs para que puedan ser rastreados por los equipos de revisión de ROSs. Nuestra incapacidad actual para identificar al tráfico humano en Internet como el delito subyacente sospechado, le hace un flaco favor a sus víctimas.

Investigaciones criminales de las víctimas

Cada vez hay más investigaciones criminales que incluyen los asesinatos de prostitutas que anunciaban sus servicios a través de avisos en Internet en la forma de servicios de acompañantes. Las investigaciones han validado que los anuncios en línea han sido atribuidos directamente a los homicidios de estas mujeres.[7] Las mujeres publicaban sus anuncios en Internet y un comprador de sexo respondía al anuncio concertando la hora/lugar para que las mujeres y el comprador se encontraran. El resultado es que las mujeres terminan siendo denunciadas por su desaparición por sus familias y las investigaciones de control legal terminan trágicamente identificando a sus cuerpos asesinados.[8] La preocupación es que al seguir la ruta del dinero, no queremos que estas víctimas que han utilizado a nuestros sistemas financieros para pagar los anuncios en Internet que pueden haber contribuido a colocarlas en estas situaciones peligrosas.[9] Con sistemas de vigilancia adecuados para monitorear los pagos de estos anuncios, los profesionales ALD pueden potencialmente tener un impacto mayor para salvar una o más vidas.

¿Cómo podemos impedir que nuestros sistemas financieros sean utilizados para lavar la venta de seres humanos?

Educación: Estar y mantenerse informado

El conocimiento por parte del investigador de las características de estos anuncios es la clave para saber cómo vigilar a estos sistemas de pago para buscar las señales de dinero que esté siendo movilizado a través de los sistemas de pago para la posible venta de servicios ilegales a través de los anuncios de Internet. Los analistas pueden monitorear la cantidad de respuestas de avisos y cancelar cualquier tarjeta que sea sospechosa. Los sitios en Internet de las organizaciones sin fines de lucro, como GEMS y Polaris son grandes recursos para la información de un investigador sobre qué está sucediendo en el comercio sexual.[10,11] GEMS, que es la sigla en inglés del sitio Servicios Educativos & de Tutoría para Niñas *(Girls Educational & Mentoring Services)* explicaba que la diferencia entre una transacción de fraude/LD y una transacción de dinero por tráfico humano es que la transacción de fraude ocurre solo una vez.[12] En tanto que, cuando una persona es vendida, las transacciones se repiten una y otra vez ya que la persona es vendida por dinero continuamente. Estos

[4] http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00957.htm
[5] http://www.fbi.gov/about-us/investigate/vc_majorthefts/cac/crimes_against_children
[6] http://www.fincen.gov/forms/files/f9022-47_sar-di.pdf
[7] http://craigscrimelist.org/2010/12/15/possible-craigslist-serial-killings-in-long-island-megan-waterman-may-be-one-of-the-victims/#
[8] http://www.irishcentral.com/news/Craigslist-is-key-to-finding-Long-Island-serial-killer-says-top-Irish-cop-119680479.html
[9] http://en.wikipedia.org/wiki/Internet_homicide
[10] http://www.sho.com/site/movies/movie.do?seriesid=0&seasonid=0&episodeid=131233
[11] http://www.polarisproject.org/what-we-do/national-human-trafficking-hotline/the-nhtrc/overview
[12] http://www.gems-girls.org/

grupos pueden ser utilizados como nuestros soldados en el campo en nuestra lucha para terminar con el tráfico de sexo desde todos los ángulos posibles.[13]

Identificación de tendencias en las tarjetas de crédito y prepagas

Una señal de alerta fundamental para los investigadores financieros es la realización de gastos múltiples en Craigslist/Backpage.com, seguidos de gastos en hoteles. Personalmente he investigado a tarjetas de crédito y tarjetas prepagas recargables que mostraban entre 20 y 30 pagos de anuncios en Craigslist/Backpage.com en un período corto de tiempo seguidos por pagos en hoteles. También analicé gastos similares en Craigslist/Backpage.com seguidos de la compra de boletos en ómnibus de la línea Greyhound, y pagos en hoteles ubicados fuera del estado de la residencia verificada del titular de la tarjeta. Cuando detecté esa actividad, entrevisté a los clientes y les pregunté si la actividad era por negocios o si era personal. Si se relacionaba con el negocio, podía cancelar la tarjeta Visa o Mastercard, privando así al titular de la tarjeta de la posibilidad de participar en la actividad de pago de anuncios en Internet. He recibido respuestas de los titulares de tarjetas que informaron que los anuncios eran utilizados para servicios de acompañantes. En un caso en el que analicé los anuncios adquiridos en Backpage.com por el titular de la tarjeta, encontré registros criminales por prostitución. Tuve conversaciones con titulares de tarjetas en los cuales una mujer dijo que alguien la iba a matar, y otro titular de tarjeta dijo que algunos esposos se habían acercado a ella porque las esposas no estaban haciendo sus tareas. Como investigador de fraude, analizo las transacciones de pagos de anuncios en Internet en las cuales mi proceso como analista es que una vez que la cuenta es identificada con 10 resultados o más de gastos en anuncios en Internet, cancelo la cuenta e inmediatamente ceso la actividad del anuncio. Investigo más solicitando que me envíen documentos de identidad por fax como la tarjeta de seguridad social, una identificación oficial con fotografía y una factura de servicios, como ser de electricidad o gas, que debe estar con el nombre y domicilio del titular de la tarjeta. Considero que esta investigación es muy productiva ya que el cliente o cumplirá con el pedido, lo cual es beneficioso para la investigación, o abandonará la cuenta. El uso de informes financieros para analizar los pagos de anuncios en Internet para detectar la posible prostitución o tráfico humano también es importante. Yo analizo un informe mensual de 10 o más resultados de anuncios en sitios de Internet que también incluyen la fecha de nacimiento del titular de la tarjeta para ayudarme a identificar si hay alguna actividad de pago de anuncios realizada por un menor de edad. Otra sugerencia para el monitoreo de la actividad es crear un código SIC para Visa y Mastercard para los sitios en línea clasificados para ayudar a facilitar las investigaciones ALD.

Hechos alarmantes

- Aproximadamente el 55% de las niñas estadounidenses que viven en la calle participa en el comercio sexual[14]
- Por cada 800 personas traficadas, solo una persona es condenada[14]
- Una niña joven pueda ganar entre US$150.000 y US$200.000 por año para su proxeneta, si sobrevive[14]
- Cada año dos millones de niños son comprados y vendidos en el comercio sexual global[14]
- La niña estadounidense promedio tiene 13 años cuando es obligada a ingresar en la esclavitud sexual comercial[14,15]
- Las víctimas de tráfico sexual también son víctimas de violaciones por parte de pandillas[16]

Nuestra responsabilidad: seguir el rastro del dinero

Es una responsabilidad del analista ALD y de riesgo vigilar a los sistemas financieros para asegurar que, de ninguna manera, nuestros sistemas financieros sean utilizados para financiar el comercio sexual de menores a través de anuncios en Internet. Es nuestra tarea identificar y reportar debidamente los delitos subyacentes del lavado de dinero. Tener relaciones sexuales con un menor es ilegal y cualquier dinero que resulte de esta actividad debería estar manchado. Asimismo, la prostitución es ilegal en muchas jurisdicciones. Colocar el dinero contaminado en el sistema financiero sería lavado de dinero y, por ende debería ser reportado en un ROS. Las transacciones de anuncios en Internet son de montos escasos en dólares para vender un anuncio con foto en estos sitios en Internet. El vendedor publicará fotos de partes del cuerpo y tratará de ocultar la identidad de la víctima en venta, como por ejemplo, una fotografía que solo muestre desde el cuello hacia abajo. Aunque los analistas pueden no ver el anuncio real, podemos identificar la actividad sospechosa por la cantidad de operaciones con ese anuncio en una cuenta, semanal o mensualmente. Detener el flujo de dinero para la publicidad ilegal de niños a la venta de sexo ayudará a reducir el comercio sexual en Internet en los EE.UU. Sin embargo, la tarea no estará completa hasta que todas las instituciones financieras y las instituciones no financieras con productos con tarjetas utilicen sistemas de monitoreo para identificar las señales de alerta de la compra o venta de prostitución en Internet. Debe entenderse que los proveedores criminales y los compradores criminales no dejarán esta actividad hasta que sus métodos de pago les sean quitados. Cuando estos canales sean interrumpidos, los criminales simplemente se trasladarán a la siguiente oferta de tarjeta de crédito o tarjeta prepagada no sospechosa.

En conclusión, nosotros como equipo antilavado de dinero podemos colaborar en la lucha para detener la venta y compra de niñas y mujeres en sitios de anuncios en Internet utilizando las herramientas financieras que tenemos para cancelar toda actividad sospechosa y reportar la actividad a través de un proceso de reporte actualizado de ROS que incluya un nuevo formulario ROS con un casillero para el tráfico humano.

Agradecimiento a la industria:

Quisiera mencionar un agradecimiento especial a Amy Wotapka, Lee Jeffrey Ross y Brian Maher por su sabiduría y apoyo.

Joann Alicea, analista de riesgo- investigaciones senior, PreCash, Inc., Houston, TX, EE.UU., joann.alicea @precash.com

[13]http://www.polarisproject.org/human-trafficking/overview;
[14]http://demiandashton.org/get-informed
[15]http://cnnpressroom.blogs.cnn.com/2011/01/18/cnn%E2%80%99s-amber-lyon-investigates-teen-trafficking-in-america/
[16]http://www.euronews.net/2011/03/08/human-trafficking-rebuilding-a-victims-trust/

Legitimate Transaction or Financial Crime?

Can You Tell?

Don't worry – you're not alone. The fact is that suspicious activity, whether part of a money laundering scheme (possibly shown above) or a scheme to defraud your bank (*also* possibly shown above), is exceedingly difficult to spot. That's why institutions of all sizes rely on the *Wiz* Sentri™ line of financial crime control solutions.

By spotlighting potential identity thieves and delivering continuous, real-time monitoring of all transactional activity and employee behavior, *Wiz* Sentri enables you to stop money laundering and fraud in its tracks – including a unique ability to detect the *potential* for loss due to fraud *before* the loss ever occurs.

Let us show you how *Wiz* Sentri can help your institution swiftly and decisively prevent, detect and investigate the complete spectrum of financial crime – contact us today.

Wolters Kluwer
Financial Services

Call 1-800-261-3111 or visit
WoltersKluwerFS.com/bankingrisk.

El vacío del monitoreo ALD – Complicidad Interna

¿Su banco o unión de crédito está ignorando uno de los mayores riesgos de lavado de dinero….la complicidad interna? Esa vigilancia puede no sorprender dada la falta general de discurso sobre cómo las actividades desde adentro pueden facilitar el lavado de dinero. Combine esta realidad con la incapacidad de los sistemas de detección de lavado de dinero para monitorear las actividades internas y obtendrá importantes riesgos que deberán ser atendidos por todas las instituciones financieras.

De hecho, el Manual del Contralor de la OCC indica que los "exámenes para detectar complicidad interna deben ser incorporados a los sistemas de control interno del banco". Además, en una "Declaración Interagencia sobre el Control Legal de las Obligaciones LSB/ALD" de 2007, la FDIC, OCC, OTS, NCUA y la FRB enfatizaron que la complicidad interna es un "factor agravante" que puede terminar en órdenes de cesar y desistir si ha disminuido la efectividad del programa de cumplimiento de la Ley de Secreto Bancario (LSB) de la institución financiera.

La OCC define a la complicidad interna en su Manual del Contralor como "la condición de ser un cómplice, socio o participación en un acto indebido". Puede ser interpretado como un esfuerzo intencional por parte de alguien interno para ayudar a los lavadores de dinero o para cometer lavado de dinero por sí mismo.

A menudo se ha demostrado que en las instituciones financieras de todos los tamaños existe un gran vacío entre las capacidades de monitoreo del equipo LSB en comparación con lo que debe monitorearse para identificar las actividades internas de fraude. Es este "vacío de monitoreo" lo que hace que sea altamente probable que las actividades de lavado de dinero cometidas por empleados/internos permanezcan sin ser detectadas durante largos períodos de tiempo. ¡Muchas señales de alerta del fraude interno no son monitoreadas en absoluto! Por ejemplo, ¿monitorea su institución para detectar la reactivación de las cuentas inactivas después de un cambio en la dirección adonde se envía el resumen; la renovación y el reemplazo de préstamos; las transacciones realizadas por empleados que no guardan relación con la descripción de su trabajo; los totales de las transacciones en efectivo diarias fuera del patrón establecido realizadas por el cajero?

Descubrir a los empleados en las primeras etapas de sus actos cómplices es crucial para evitar o mitigar el impacto severo sobre la institución financiera como:

- Daño reputacional
- Multas y sanciones
- Confusión interna importante
- Posibles préstamos irrecuperables a causa del decomiso de bienes
- Consideración del regulador por la emisión de una Orden de Cesar & Desistir

Ejemplos de complicidad interna

Existen muchos esquemas de fraude interno y de escenarios relacionados que pueden cometerse contra su institución en un intento por ocultar las actividades de lavado de dinero (LD). ¿Cuántos de los esquemas descritos a continuación podrían suceder en su institución sin ser detectados durante un período de tiempo extenso?

A. Esquemas internos minoristas

Su "línea frontal de defensa" puede verse comprometida por esquemas como los siguientes:

- *Apertura de Cuenta Fraudulenta* — Alguien interno podría fácilmente hacer aparecer que un cliente, sin identificación aceptable, entregó una identificación aceptable. La obtención de la identificación correspondiente es un componente fundamental requerido por los estándares del Conozca Su Cliente de la LSB/Ley Patriot USA.
- *Estructuración* — Alguien interno ayuda a un cliente a estructurar depósitos o hace como que no ve cuando el mismo cliente hace depósitos frecuentes de dinero en efectivo en cuentas aparentemente no vinculadas. ¡Los individuos que trabajan en las instituciones están apareciendo como empleados que reciben sueldos de los lavadores de dinero con mucha más frecuencia en la época actual!
- *Cuentas ficticias* — Alguien interno puede realizar su propio esquema de lavado de dinero, o trabajar con un cómplice abriendo cuentas de depósitos ficticias y/o de hecho apoderándose de cuentas inactivas. Por ejemplo, si solo se depositaran US$2.500 en efectivo por mes en diez cuentas distintas, alguien interno podría lavar más de US$300.000 al año. Las sumas depositadas mensualmente probablemente serían elegidas deliberadamente por debajo del monto mínimo sujeto a monitoreo por la institución.

B. Esquemas de internos de la oficina de apoyo

Hacer cambios innecesarios al sistema automático de detección de LD también genera un enorme área de riesgo. Los controles y el monitoreo del sistema automático de detección de LD necesitarían ser extremadamente ajustados para detectar estos eventos, especialmente dado que los ingresos al sistemas pueden ser manipulados.

- *Parámetros mínimos en dólares* — Los internos que participan en el monitoreo de la actividad de LD pueden modificar los montos mínimos en dólares en el sistema de LD durante un plazo temporario de tiempo para hacer que determinadas transacciones no sean detectadas.

… el Manual del Contralor de la OCC indica que los "exámenes para detectar complicidad interna deben ser incorporados a los sistemas de control interno del banco"

- *Excepciones no calificadas* — Los internos que clasifican a los clientes no calificados como "exceptuados" directamente en el sistema de detección de LD para eludir el reporte, y luego los "devuelven" al estado de "no exceptuado".
- *Parámetros de las transacciones* — Los internos establecen los parámetros del sistema de LD para ignorar determinadas transacciones en efectivo durante un período de tiempo, luego los "cambian" y vuelven al parámetro correcto. Los reguladores esperan que las instituciones financieras realicen una conciliación del dinero en efectivo para demostrar que el sistema detecta todas las transacciones en efectivo. ¿Su institución está haciendo esto?

C. Esquemas de internos relacionados con préstamos

Los préstamos a menudo están vinculados con el lavado de dinero:

- *Préstamos fraudulentos* — Estos préstamos hechos por empleados de la institución a menudo llevan a la presentación de acusaciones de lavado de dinero por parte de las agencias de control legal. Una vez que el interno trata de ocultar el origen de los fondos obtenidos ilegalmente con un préstamo fraudulento, generalmente a través de prestatarios intermediarios o terceros, el delito también se convierte en lavado de dinero. A veces, las compañías "pantalla" son utilizadas en estos esquemas, y es común que el banco asuma como pérdidas millones de dólares utilizados en estos esquemas.
- *Préstamos con "rápidos pagos a cuenta"* — Estos son un posible indicador de préstamos relacionados con actividades de lavado de dinero. Sin embargo, los sistemas automáticos de detección de LD normalmente no tienen la capacidad de identificar las anomalías en los repagos de préstamos, que pueden no ser en efectivo, y las fuentes de esos fondos.

D. Esquemas de internos en la gerencia

Siempre debería mantenerse un nivel de concientización respecto de la capacidad de la gerencia de anular los controles:

- *Anulación por parte de la gerencia de los Controles Internos Existentes* — La gerencia puede presionar a los empleados para que infrinjan varias políticas y procedimientos LSB. Por ejemplo, podrían exceptuar el reporte de Reportes de Transacciones en Efectivo (RTE) de determinados negocios que sean propiedad de amigos y asociados que normalmente no calificarían para las excepciones o entregar estados financieros fraudulentos para respaldar esos pedidos. Dado que la gerencia está en posición de aprobar esas excepciones, existe una necesidad imperiosa de monitorear para detectar cualquier acción indebida.

> Según la Asociación de Examinadores de Fraude Certificados, las auditorías internas y los controles internos son muy limitados para detectar y prevenir el fraude

¿Qué debería hacer?

Según el Manual del Contralor de la OCC, su institución financiera debe tomar las siguientes medidas para prevenir y detectar la complicidad interna:

- Implementar un estricto proceso de vigilancia de empleados
- Revisar las cuentas y estilo de vida de los empleados clave, especialmente de aquellos asignados a áreas y cuentas de mayor riesgo
- Asegurar que los controles internos incluyan la complicidad interna de manera constante
- Examinar la complicidad interna como parte del programa de auditoría interna

Para asegurar que los controles internos incluyan la complicidad interna de manera constante, debería analizarse la realización de una evaluación de riesgo de fraude para identificar los esquemas específicos a los cuales puede estar más expuesto, luego implementar un nivel adecuado de controles y/o incremento del monitoreo.

Cómo detectar — Monitorear es la clave

Según la Asociación de Examinadores de Fraude Certificados en su "Reporte a las Naciones sobre Fraude y Abuso Ocupacional" de 2010, las auditorías internas y los controles internos son muy limitados para detectar e impedir el fraude. Por lo tanto, la clave para combatir la complicidad interna es no descansar sobre los controles internos, sino crear un programa sólido independiente de monitoreo de fraude interno. Sin ese programa la integridad del programa LSB de la institución podría ser cuestionado. El programa debería estar integrado por los procesos manual y automático y estar diseñado para encontrar todo tipo de actividad sospechosa.

Existen varios programas de software de análisis de fraude disponibles, conocidos también como herramientas de computación de auditoría asistida (CAATs, por sus siglas en inglés). Ellos incluyen rutinas analíticas de información y capacidades de análisis de datos para detectar muchas de las señales de alerta que son consecuencia de esquemas de complicidad interna.

Las herramientas más efectivas incluyen análisis que son mapeados directamente en el sistema bancario principal de la institución financiera. Estas herramientas pueden en muchos casos detectar cuentas ficticias, control de cuentas, préstamos fraudulentos, anomalías en la identificación de clientes, actividad inusual de depósitos en las cuentas de empleados, anomalías en el reporte de dinero en efectivo, así como también varias otras señales de alerta. Podrían detectar muchos de los ejemplos de complicidad interna mencionados en este artículo.

Resumen

Los lavadores de dinero siempre están buscando el camino de la menor resistencia. ¡Ese camino puede muy bien estar dentro de su institución! No importa cómo monitoree el fraude interno, simplemente recuerde que debe ser dirigido de manera efectiva, y con miras al lavado de dinero.

Dado que muchas instituciones han resuelto que sea imperioso combinar sus funciones ALD y de fraude externo, también deberían considerar agregar el monitoreo del fraude interno. Ello brindaría una visión amplia de todas las actividades sospechosas a nivel general de la empresa e indudablemente revelaría más eventos vinculados, de alto riesgo, ¡cerrando así el fundamental vacío de monitoreo ALD!

Robert P. Jones, CFE, principal, Risk Consultants Group, LLC, Dracut, MA, EE.UU., RobertJonesCFE@comcast.net

Stephen O. Friend, CAMS, Vicepresidente, Sales, Focus Technology Group, Danvers, MA, EE.UU., Stephen.Friend@FocusTechnologyGroup.com

¿Adónde han ido a parar todas las células dormidas?

Nosotros como sociedad marcamos el paso del tiempo y los hitos en nuestras vidas cada cinco años, como nuestro 25to. aniversario de bodas o nuestro cumpleaños 50. Este septiembre, Estados Unidos conmemorará una clase diferente de aniversario, el décimo aniversario del 11/9. Para muchos, los horrendos eventos de ese día, que cambiaron la vida de millones de personas para siempre, están todavía grabados indeleblemente en la memoria como si hubiera sucedido ayer. Para la generación de los *baby-boomer* cristalizó la emoción y la psiquis que la nación debe haber sentido después de Pearl Harbor, algo que los libros de textos, las películas y los relatos escritos nunca pueden reproducir totalmente.

El 11 de septiembre de 2001 inició el despertar de los esfuerzos de la Ley de Secreto Bancario (LSB) y antilavado de dinero (ALD), presentando un nuevo vocabulario al léxico estadounidense a lo largo de los años posteriores. Palabras y frases como reporte de operación sospechosa (ROS), programa de identificación de cliente (PIC), conozca a su cliente (CSC), simulacro de ahogo *(water boarding)*, avión no tripulado y célula dormida son ahora términos que ya no están reservados para las discusiones secretas en los niveles más altos del gobierno. De todos esos términos, el de células dormidas es uno de los que generó que el gobierno y el sistema financiero se movilizaran por el miedo generado en septiembre de 2001, algo parecido a una Guerra de los Mundos descendió sobre los Estados Unidos.

Miedo a lo desconocido

La célula dormida es la personificación psicológica del miedo. Es terrorismo menos el acto terrorista. Mientras que el atacante suicida con bombas genera un miedo que reacciona más exteriormente, la gente no está muy segura de cómo reaccionar con relación a la célula dormida. La diferencia entre los dos es que un acto de violencia premeditada no es para nada inusual en los Estados Unidos, pero la idea de que personas que viven entre nosotros durante una década o más tiempo, comentan luego ese acto, pueden dejar un miedo emocional profundo. Las preguntas siempre nos atormentarán. ¿Por qué no los pudimos descubrir? ¿Por qué no hicimos más? La idea de que en este mismo momento puede haber varios individuos en los Estados Unidos, Canadá y Europa, que un día pueden ser llamados a las armas, no solo es desconcertante, sino que genera un sentimiento de total frustración.

Misión imposible

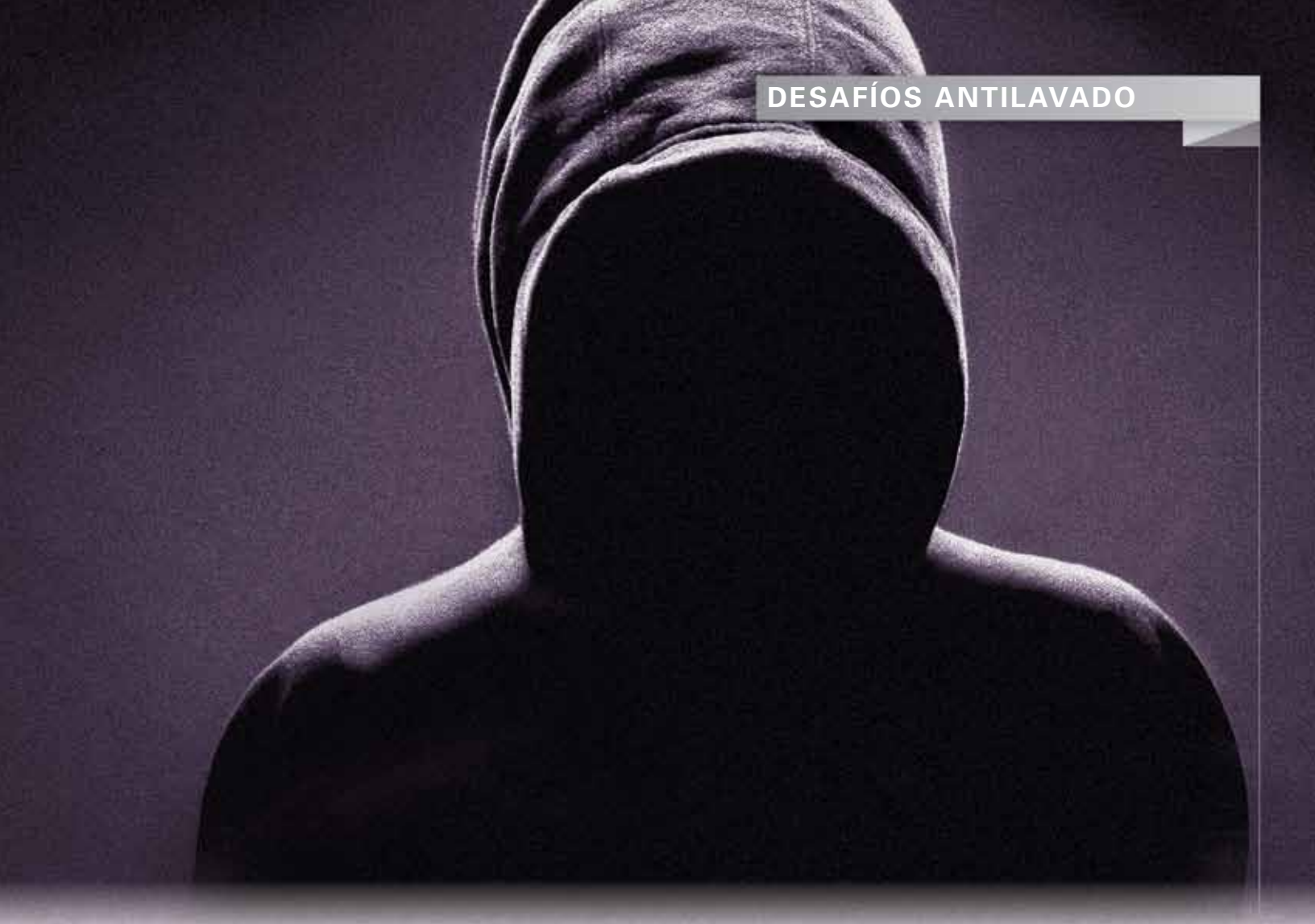
Todos sabemos que las posibilidades de descubrir información del lado de las instituciones financieras que lleven directa o indirectamente a descubrir una célula dormida es incluso mayor que el proverbio de buscar una aguja en un pajar. Cualquiera que diga lo contrario está alucinando o está tratando de impresionarlo. Las células dormidas pueden ocultarse durante una década o más de cultural occidental normal, o pueden haber nacido aquí y convertirse con el transcurso del tiempo. El perfil original de la célula dormida de un hombre del Medio Oriente que es un solitario, anda con prostitutas y tiene un trabajo nada calificado o es un estudiante, fue un acto reflejo en ese momento. Descartemos el aspecto étnico y el perfil encaja en millones de hombres. Si incluimos lo étnico, más la información que las instituciones financieras conocen, y el objetivo grupal se reduce considerablemente. Encontrar a un posible terrorista; o tal vez, e igual de importante a un simpatizante de los terroristas, requiere tirar por la borda el libro con todas las jugadas de señales de alerta ALD usuales y trascender los informes normales que indagan la superficie del crimen económico.

Análisis de tarjetas de débito/crédito

Los análisis estadísticos de las compras de tarjetas de débito y crédito es tal vez la columna vertebral del mercadeo de productos al consumidor. Cuando se los combina con los depósitos y los cheques escritos, el banco puede elaborar un perfil de un individuo que competiría con uno agente del FBI cuya especialidad sea elaborar perfiles (incluso con información que ni siquiera el cónyuge puede desconocer. Un individuo que compra cantidades extraordinarias de comida, productos de higiene personal, productos para bebé, teléfonos celulares prepagados o gasolina, es ciertamente indicador de alguien que posiblemente se ocupe de otros. Si es un clérigo, por ejemplo, puede ser nada más que una causa noble, como un centro para adolescentes con problemas. Por otro lado, también podría ser un signo de gente que vive aquí ilegalmente en la forma de servidumbre, tráfico humano o terrorismo. Forma parte de la naturaleza humana que en cualquier estructura, sea que se trate de una familia, el ejército o una célula terrorista, se le asignen tareas a los integrantes de esa estructura, para dar apoyo a todo el grupo como un todo.

Análisis de direcciones cruzadas

Realizar la verificación de una dirección cada seis meses para ver cuántos individuos (especialmente no relacionados) están residiendo en la misma casa puede revelar una situación prejudicial que está esperando para suceder. Seis hombres viviendo en una dirección que se sabe o es un lugar común que es un departamento de un dormitorio o que debería generar preguntas sobre qué hace el grupo. Dado que los bancos más pequeños tienen restricciones en áreas geográficas de servicios, podría ser algo tan benigno como un grupo de amigos muy unidos tratando de aprovechar la ventaja de utilizar la tasa promocional del certificado de depósito,



usando la casa de uno de los participantes como pantalla. También podría ser un grupo que participe en una variedad de esquemas fraudulentos, lo que requiere una revisión inmediata de los documentos del PIC junto con una investigación.

Hawala

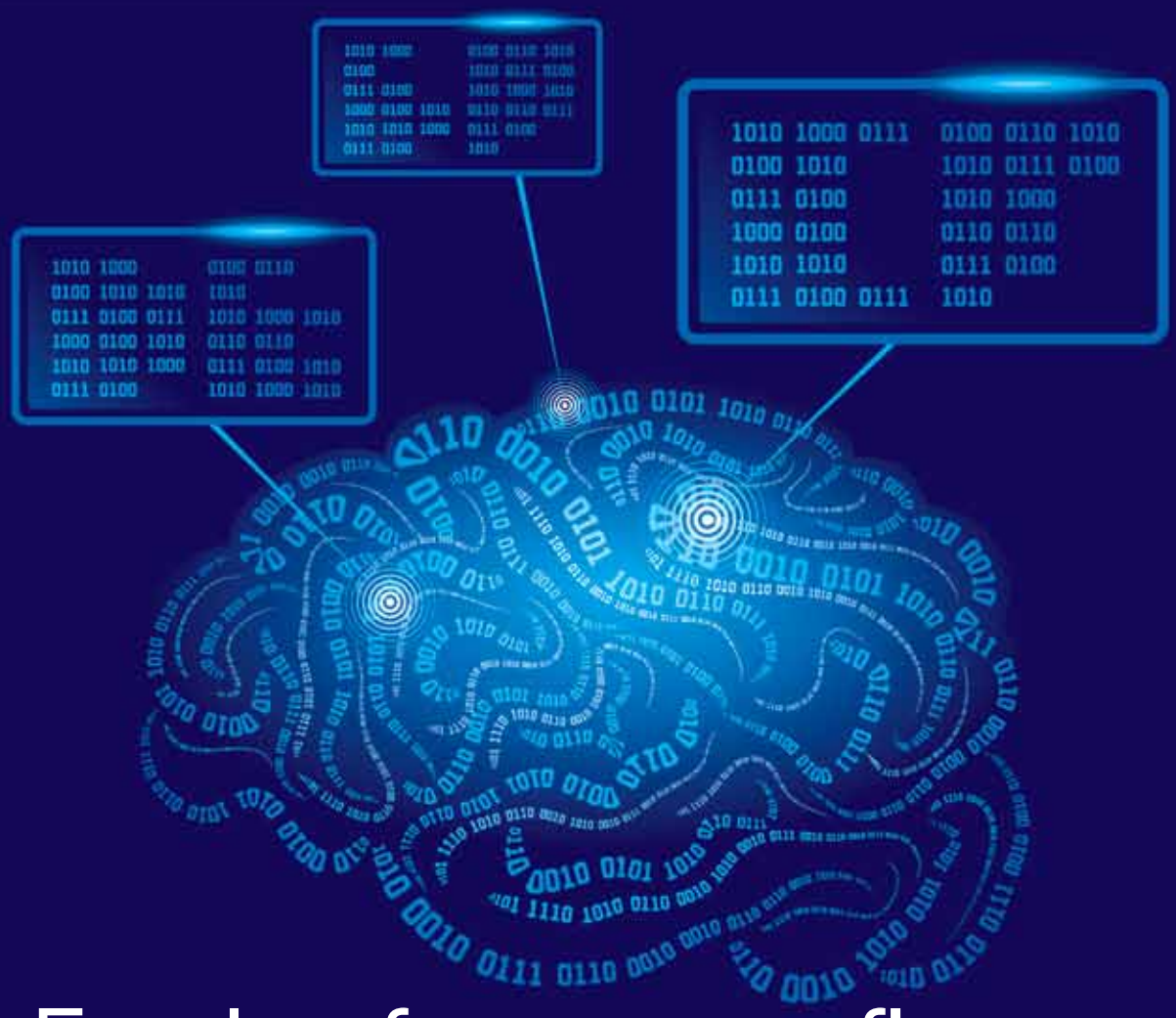
Descubrir a alguien que participe en hawala es ciertamente de gran interés para las autoridades de control legal. La preponderancia de individuos involucrados en este tipo de banca alternativa es desde lejos inocua desde el punto de vista del terrorismo, pero esa una decisión que es mejor dejar para las autoridades de control legal. La mayoría de la gente utiliza el hawala para simplemente enviar fondos a familiares en el exterior y para empezar puede no tener ninguna relación bancaria. El hawaladar (el broker del hawala) es la clave, el descubrirlo es el eje de una posible mina de oro de información. Dado que muchos hawaladares operan un negocio legítimo con servicios bancarios tradicionales, se aplican las señales normales de alerta de lavado de dinero, como un depósito seguido de una transferencia al exterior por el mismo monto. Hay que prestar especial atención a los depósitos de cheques no relacionados con el negocio caracterizado por anotaciones en el espacio del memo que tampoco están relacionadas. Los cheques personales depositados fuera de los Estados Unidos también pueden ser indicadores de una transacción con hawala.

Depósitos vendidos con descuento

Los depósitos que llegan a una cuenta comercial a través de un intermediario son extremadamente inusuales porque esos depósitos son más inusuales cuando el negocio no es el tipo de empresa que necesitaría contar con un servicio de intermediario (como por ejemplo un negocio con gran manejo de efectivo). El factoring es la venta de cuentas a cobrar con descuento a cambio de un pago en efectivo inmediato. Los pagos de un factor ciertamente dan la apariencia de legitimidad, dando una cobertura excelente para que una empresa criminal movilice el dinero. Si bien el acuerdo de factoring puede establecer que sea abierto u oculto, el resultado final es que a través de las facturas falsas, o una serie de compañías pantalla y/o compañías legítimas (que pueden incluir a la compañía de factoring), un negocio puede ocultar sus depósitos de las instituciones financieras. Como se mencionó anteriormente, las preguntas clave a realizar son por qué el negocio en cuestión necesita contar con el factoring y, por supuesto, ¿cómo son desembolsados esos depósitos?

Si bien la muerte de Osama Bin Laden puede producir alivio, el terrorismo ha existido mucho antes de que escucháramos hablar de Osama Bin Laden. Sea que se trate de secuestros de aviones, el Achille Lauro, la Olimpíadas de Munich o Entebbe, la historia ha demostrado que nunca hay poca gente mala esperando atacar a la humanidad por cualquier razón ilusoria que los posea. Todos ellos comparten una cosa en común, la necesidad de tener fondos para sus complots y para que sus seguidores se puedan infiltrar.

Charles Falciglia, CAMS, Suffern, N.Y., EE.UU., charlesfalciglia@yahoo.com



En el software confiamos — ¿confiamos?

Una tendencia actual creciente en las iniciativas regulatorias globales es el incremento de la carga sobre los bancos y otras instituciones para asegurar que sus programas de cumplimiento antilavado de dinero (ALD) no solo sean sólidos, sino que también hayan sido puestos a prueba. El mensaje de los reguladores por el incumplimiento con las regulaciones de la OFAC, la LSB y la Ley USA Patriot es muy claro: multas enormes, vigilancia intensa y obligaciones adicionales de monitoreo.

Más obligaciones significan más diligencia debida. Más diligencia debida aumenta la cantidad de alertas y consecuentemente lleva a un aumento de las falsas alarmas. A pesar de la automatización, la administración de alertas continúa siendo un desafío monumental para la filtración de las listas de vigilancia — uno oneroso para ello. Los costos cada vez mayores del análisis manual y la determinación de cuáles alertas requieren una investigación adicional agravan el problema.

Sin perjuicio de su tamaño, los reguladores esperan que todas las instituciones apliquen controles y tecnologías efectivas y eficientes para monitorear a los clientes y las transacciones. Si bien las instituciones trabajan para optimizar sus procesos basados en el riesgo, los proveedores de software en este mercado han dedicado años a desarrollar algoritmos y lógicas basadas en reglas para ayudar a administrar las "fábricas de alertas". Pero este enfoque, que se concentra principalmente en la cantidad y no en la calidad de los alertas, es insuficiente. Todavía quedan demasiados alertas que las instituciones deben manejar de manera oportuna. No obstante, los bancos y otras instituciones han adoptado decididamente estas soluciones de software. Si bien no resuelven completamente el aluvión de alertas, sí facilitan el cumplimiento con las

obligaciones de conozca a su cliente (CSC), diligencia debida reforzada (DDR) y monitoreo de transacciones.

La espada de doble filo de la menor cantidad de alertas

"Reduzca las falsas alarmas y mejore el desempeño del investigador". "La disminución de las falsas alarmas es fundamental para lograr la eficiencias en el monitoreo de las sanciones y las personas expuestas políticamente (PEPs)". "Reducir la carga de trabajo con menos falsas alarmas". ¿Cuántas veces ha leído estas declaraciones en un folleto de comercialización o las ha escuchado en un puesto de ventas? Es casi imposible analizar la filtración de las listas de vigilancia sin mencionar las falsas alarmas. ¿O no es así?

Estamos empezando a ver que el foco de atención sobre la reducción de la cantidad de alertas está teniendo consecuencias no deseadas de maneras que ni las instituciones, los reguladores ni los proveedores de software jamás anticiparon. En un ámbito de intenso escrutinio regulatorio, generar "demasiado pocos" alertas puede hacer que la gerencia superior y los reguladores sospechen que algo no está siendo detectado. Como resultado de ello, las instituciones dudan al establecer dónde fijar sus límites mínimos de filtración y están reevaluando sus niveles de riesgo. Si los límites mínimos de filtración son establecidos demasiado altos generando pocos alertas, surge la preocupación de que el sistema no esté identificando de manera efectiva el riesgo. En consecuencia, los alertas importantes no serán realmente detectados. Si se lo fija demasiado bajo y la filtración genera una sobreabundancia de alertas de baja calidad, consumirán valiosos recursos para la investigación, mientras que los alertas potencialmente de alto riesgo seguirán estando al final de la pila.

Reducir las falsas alarmas y la cantidad general de alertas, una vez eliminada la mitigación del riesgo, genera súbitamente cuestionamientos. Por lo tanto, debemos preguntarnos si una alternativa que también considere la calidad de los alertas como factor principal puede ser un enfoque más efectivo para administrar el riesgo.

Marcando una nueva dirección

Hasta ahora, los examinadores regulatorios, han estado expuestos a una variedad de soluciones de filtración de listas de vigilancia al realizar sus inspecciones y han ideado tests rígidos para la identificación exacta de nombres para evaluar la efectividad del software de cumplimiento de una institución. Se espera que la institución bajo análisis conozca la aplicación del software. Las instituciones deben poder articular cómo se adapta y qué metodología utilizan para establecer si un resultado es verdadero o falso.

La tecnología se basaba en una principio matemático y científico para obtener conclusiones sobre la posibilidad de que una alerta sea verdadera puede tener un impacto tremendo en la capacidad de la institución no solo para administrar el riesgo de manera efectiva y eficiente, sino también para demostrar un programa de cumplimiento eficiente. ¿Una visión del futuro? Todo lo contrario. Representa un nuevo paradigma que ha logrado su camino haciendo que las instituciones se anticipen a ello, con una visión holística de la administración del riesgo.

El uso de elementos específicos de información para calificar la relativa fortaleza de las posibles coincidencias obtenidas por un filtro y luego corroborar esta información con otras fuentes de información le da facultades a las instituciones para priorizar aquellos alertas que tengan más posibilidades de ser verdaderos. La gran mayoría de las falsas alarmas obtenidas con software en la coincidencia de nombres puede ser luego eliminada utilizando puntos de conflicto para eliminar las coincidencias sin necesidad de intervenciones manuales. Los límites de riesgo están definidos claramente y el analista de cumplimiento ahora tiene una preponderancia de evidencia que respalda la calidad del alerta.

Generando confianza

Desafiar el status quo y cambiar la manera en que los profesionales de cumplimiento consideran a la administración de alertas podría ser considerado un acto audaz en una industria tradicionalmente conservadora. Pero, ¿pueden las instituciones esperar realmente mantener el ritmo con los lavadores de dinero, los defraudadores y quienes cometen otros delitos financieros si continúan eligiendo el camino de la resistencia menor?

La naturaleza dinámica del ALD, el fraude y el cumplimiento y sus obligaciones regulatorias, junto con el eterno problema de tener demasiados alertas, es razón suficiente para buscar socios tecnológicos cuyas técnicas de reducción de alertas estén diseñadas alrededor del nuevo paradigma y ya estén probadas en escenarios del mundo real con resultados demostrados.

La siguiente guía le ayudará a facilitar una evaluación adecuada y lograr la confianza:

- Solicitar una prueba de concepto para medir los resultados contra las mediciones actuales
- Validar que los procesos de vigilancia sean consistentes y respetables
- Verificar la relevancia de los alertas priorizados
- Aplicar varios escenarios para determinar la tolerancia al riesgo
- Conocer cómo se adapta el software y el posible impacto en distintos escenarios y límites
- Asegurar que la metodología sea defendible ante los reguladores
- Generar una relación de confianza con el proveedor que esté abierta al intercambio de conocimientos

El siguiente paso es educar a la gerencia superior, los reguladores y otros sobre que el objetivo de lograr menos alertas aún sigue siendo válido pero solo si el foco de atención está en la generación de alertas que sean tanto de alta calidad como relevantes. Las mediciones confiables recibirán su confianza en la validez y el éxito de este enfoque.

Un buen programa ALD y de cumplimiento debe demostrar su habilidad para ejecutar un plan. Esto requiere una infraestructura operativa que combine tecnología con inteligencia humana. No hay dudas de que la primera línea de defensa de una institución para combatir el crimen financiero y protegerse contra el riesgo reputacional, financiero y operativo es el personal bien entrenado que conoce los matices de las aplicaciones que utilizan diariamente. Es igualmente importante una cultura dentro del cumplimiento en todos los niveles que desee cuestionar el status quo y aceptar soluciones nuevas para viejos problemas. Y finalmente, las sólidas relaciones de trabajo con los socios tecnológicos generan el respeto y la confianza mutua de que el software recibido hace lo que se supone debe hacer.

Carol Stabile, CAMS, gerente de negocios senior, Safe Banking Systems LLC, Mineola, NY, EE.UU., carol.stabile@safe-banking.com

Una paranoia (in)salubre

Andy Grove, el fundador y ex CEO de Intel, dijo genialmente, "Solo lo paranoico sobrevive". También escribió un libro sobre negocios con el mismo título. ¿Existe una prueba de que la paranoia ha llegado al departamento de Cumplimiento y, si es así, es eso algo bueno?

¿Una (perforación) demasiado lejos?

Existen varios casos de estudio recientes que plantean lo contrario; tal vez los oficiales de cumplimiento no son lo suficientemente paranoicos. Considere el caso de Transocean, la compañía suiza que provee equipos de perforación para la exploración de petróleo y gas natural. La empresa firmó un acuerdo con CNOOC, la empresa estatal china de energía, para proveer la plataforma de perforación *Actinia* para la exploración en las afueras de las costas de Myanmar. Sin embargo, CNOOC se había asociado con China Focus Development. Esta firma, conocida anteriormente como Golden Aaron, es propiedad total de Steven Law (también conocida como Tun Myint Naing) y su esposa Cynthia Ng (también conocida como Ng Sor Hong). Law y Ng están incluidos en la lista de Nacionales Especialmente Designados (SDN, por sus siglas en ingles) de la OFAC por su participación tanto en la junta militar en Yangon y en el tráfico de drogas en el sudeste asiático.

Si bien Transocean tiene oficinas en los EE.UU. en Houston, Texas, la empresa alega que no estaba en infracción porque el nombre de Law no aparecía en el contrato firmado con CNOOC. También argumentaba que, dado que *Actinia* es un buque panameño y que Transocean es una compañía suiza, la transacción no estaba sujeta a la supervisión de los EE.UU. ¿O si? Ciertamente, si el contrato fue negociado aisladamente y la transacción fue realizada en las oficinas suizas donde trabajan 12 personas, la OFAC no podría multar a la empresa, ya que "ninguna persona de los EE.UU." habría participado en la firma del contrato.

El primer reclamo de la compañía señala una falta de rigor de cumplimiento. La diligencia debida de los socios comerciales se extiende a los dueños beneficiarios de esas empresas. Para darle a Transocean algún crédito, China Focus Development no está incluida en la lista de SDN. Sin embargo, una revisión

superficial del sitio en Internet de CNOOC menciona el cambio de nombre y que Golden Aaron aparece en la lista de SDN.

El segundo argumento de Transocean, si bien es potencialmente válido, no capta el punto principal. Aún si pudiera suministrarlo si no estuviera sujeto a una sanción civil, la compañía podría, en teoría, terminar ella misma en la lista de SDN. Tal vez, un cálculo cínico tenido en cuenta en el proceso de pensamiento de la compañía: ¿Sancionaría el gobierno de los EE.UU. a una empresa tan esencial para la industria energética de los EE.UU.? Esa es una gran apuesta, especialmente a la luz de las cifras en dólares involucradas; la empresa cobraba US$206.000 por día de alquiler del *Actinia*.

Sin forma de barco

En 2010, Maersk, una de las empresas de transporte marítimo más grande del mundo, fue multada en aproximadamente US$3,09 millones por violaciones a las sanciones iraníes y sudanesas. Maersk es una empresa dinamarquesa, pero algunos de sus buques tienen bandera estadounidense, lo que hace que esos buques estén sujetos a las regulaciones estadounidenses.

En general, la empresa había tomado todos los recaudos. Los buques que atracaban en Irán no eran buques de carga de los EE.UU., y la compañía había recibido licencias de la OFAC específicas para embarques de ayuda alimenticia para Sudán.

Donde Maersk estaba en conflicto con las regulaciones de los EE.UU. no era en no tener sistemas y controles relacionados suficientemente detallados. Los embarques iraníes, a pesar de no incluir mercaderías de los EE.UU., estaban sujetos a la vigilancia de la OFAC porque eran transbordados en buques de los EE.UU. Sistemas de cumplimiento mejores habría detectado el conflicto antes de que ocurriera y habrían hecho que Maersk asignara otros buques para la transferencia de la carga.

Asimismo, si bien los embarques de alimentos estaban autorizados, también se había enviado una carga adicional a Sudán. Los sistemas y controles mejorados podrían haber cambiado las mercaderías no autorizadas a buques no estadounidenses.

¿Está el zapato en el otro pie?

De manera que éstos son los casos donde empresas lo suficientemente grandes como para conocer mejor la situación, no supieron y consideraron al cumplimiento en un contexto demasiado limitado. El pecado de Transocean fue no ir lo suficientemente lejos en investigar los antecedentes de sus socios comerciales, mientras que la falla de Maersk en la planificación y seguimiento de sus embarques con más detalle le generó una sanción civil importante.

¿Existe también el problema opuesto? En otras palabras, ¿existe evidencia de un cuidado excesivo — arrojar redes más y más amplias en un esfuerzo inútil por identificar algo que remotamente pudiera generar una señal de alerta, sin importar si representa una violación real, y mucho menos una que genere un escrutinio regulatorio?

Solo a nombre

Recientemente, varios bancos de la Franja 1 pidieron una lista de los 100 nombres birmanos más comunes para tratar de identificar las transferencias hacia Myanmar. Estas empresas habían notado que, cada vez con más frecuencia, había referencias a individuos birmanos que omiten detalles del domicilio con la ciudad y el país. Estos esfuerzos por evadirse son consistentes con otros esquemas, como la designación de empresas birmanas con nombres occidentales comunes (p.e., empresas de Nueva York y Hong Kong con sede en Yangon). Los bancos justifican el pedido por razones de costo indicando que los nombres birmanos son razonablemente únicos y que no hay tantas posibilidades de confundirlos con los de otras personas.

Existen dos problemas con este esquema directo. La primera razón de que un esfuerzo tan grande para detener las transacciones birmanas sea desacertado es que ninguno de los programas de sanciones más importantes impuestos sobre Myanmar, incluidos los de la Unión Europea y los Estados Unidos, establece una prohibición total sobre los negocios con el país y sus ciudadanos. Las sanciones de la OFAC, por ejemplo, permiten explícitamente las transferencias financieras desde Myanmar hacia los EE.UU. y las remesas personales para aquellos que no estén expresamente incluidos en la lista de SDN o descriptos en el folleto de las sanciones. Al establecer un estándar más elevado, estas empresas incurren en costos operativos mayores y posiblemente rechacen negocios legítimos. ¿El incumplimiento de las entidades que figuran en la lista, tal vez mejorado por proveedores de información comercial para incluir las categorías de personas especificadas en el folleto de sanciones, no sería una manera más específica de solucionar el mismo tema?

El segundo tema es uno de carácter moral: ¿es este un esfuerzo bien intencionado para vencer a un esquema más sofisticado de evitar la detección o está al borde de hacer un perfil racial? ¿Tendría un individuo birmano no residente un recurso si sus transacciones comerciales se vieran demoradas, exclusivamente sobre la base de que tienen un apellido común? Seguramente, si se aplicaran esfuerzos equivalentes para identificar a gente con nombres musulmanes o hispanos, el alboroto que eso generaría rápidamente anularía esos esfuerzos.

Consecuencias adversas

Una segunda tendencia que limita con la extralimitación es el escrutinio de fuentes de noticias para encontrar historias con repercusiones negativas. Muchas empresas, como parte de sus procesos de Conozca a Su Cliente (CSC) al incorporar a nuevos clientes o pedir información a los ya existentes, explora noticias adversas en los medios para identificar a clientes indeseables. Todos los proveedores de información más importantes participan en una carrera de armas de toda cada por estas informaciones; la cantidad de fuentes de información se ha convertido en un punto de ventaja competitiva.

¿Cómo podría ser esto algo malo? ¿En qué punto no es negación de servicios — o incluso la justificación del cobro de una prima basada en el riesgo?

Los oficiales de cumplimiento argumentarán que alguien bajo investigación como mínimo requiere un mayor monitoreo. ¿Eso no depende, sin embargo del tamaño y alcance del delito? ¿No depende también de la calidad de la fuente? ¿Los profesionales de cumplimiento conocen lo suficiente para evaluar la veracidad de las decenas de miles de sitios de noticias que entregan esas historias (según uno de los mayores proveedores de medios adversos)? ¿Y cuál es el costo de descartar noticias en el medio de las enormes cantidades de coincidencias de falsas alarmas?

El problema, de paso, no es realizar análisis exhaustivos de medios adversos para sus clientes, o de tratar de ver cuáles aparecen en las bases de datos de Personas Expuestas Políticamente (PEP). El problema es realizar esas actividades para todos los clientes, sin tener en cuenta otros riesgos. Si un cliente es de alguna manera un cliente de bajo riesgo, ¿la mayoría de las historias adversas publicadas en la prensa afectarán materialmente la manera en que es administrada su relación?

Hay otros ejemplos de cómo, cuando los oficiales de cumplimiento tienen una herramienta nueva y reluciente, existe un deseo abrumador de analizar todo detalladamente.

A veces, inocente o maliciosamente, la información aparece en el lugar equivocado en una transacción comercial. Mientras que el nombre de una compañía puede aparecer en un campo correspondiente a "nombre", la información "al cuidado de" puede aparecer en el campo de la dirección, debido a una falta de campo separado para esa información. Otras veces, dos partes aparecerán en un mismo campo debido a la falta de sofisticación en el otro extremo. Y, sí, hay veces en que la información sensible es enterrada en un campo donde el remitente espera que el receptor no revise. Revisar estos episodios raros, sin embargo, es caro; una revisión de la actividad ACH transfronteriza de un importante banco de los EE.UU. mostró que más del 40% de los registros que requerían revisión tenía coincidencias con las listas de sanciones regulatorias en esos campos.

Hay una resistencia a limitar el alcance de esas actividades, aún cuando se presenten con pronunciamientos regulatorios sobre los programas basados en el riesgo. En el último mes, el banco estadounidense mencionado anteriormente que revisaba el tráfico ACH y un importante banco internacional han indicado que cualquier respuesta regulatoria no es aceptable para ellos. Las empresas querían incluso evitar recibir una advertencia, como una Carta de Advertencia de la OFAC, que no acompaña un resultado público o una sanción civil. El estar dispuesto a incurrir en importantes costos operativos constantes a fin de evitar una "consecuencia" sin importancia parece más consistente con la paranoia que con la administración adecuada del riesgo.

Moderación en todas las cosas

Entonces, ¿están los profesionales de cumplimiento administrando el riesgo — o solo están tratando de evitarlo? En el escenario actual, ¿el foco está en evitar que se cometan incluso hasta delitos menores a nuestra vista?

Tal vez pueda aprenderse una lección de la industria de seguros. El precio de las pólizas de seguros se basa en factores estadísticos y demográficos; los conductores jóvenes pagan más por el seguro del automóvil porque tienen más probabilidades de tener un accidente, mientras que la gente de más edad paga más por las primas de seguro de vida porque sus pólizas tienen más posibilidades de ser cobradas durante el plazo de la póliza. Una aseguradora de los EE.UU. con visión de futuro ofrece un dispositivo para monitorear los hábitos de manejo para que los clientes de más bajo riesgo puedan demostrar su mérito para pagar menores tarifas.

> El truco es saber cuándo un evento desapercibido pasa a tener una importancia que puede ser ignorada y cuándo requiere nuestra atención

¿Qué nos dice esto? Tal vez el nivel de verificación del cumplimiento aplicado a una relación o una transacción debería estar en proporción con el posible riesgo que representa el cliente. Un cliente que solicita una línea de crédito de US$50.000 probablemente no requiera una revisión de los medios periodísticos adversos. Y, tal vez, un crédito ACH transfronterizo de US$250 no requiera buscar a los malos en los campos existentes para indicar el domicilio, o de referencias sobre los buques de carga iraníes.

(Descargo de responsabilidad: todo esto depende de la mentalidad de su regulador y de la transparencia con que actúen. Una conversación con alguien que acepte escucharnos sería fructífera en los casos donde esas respuestas no son claras.)

Si existe un deseo de mostrar un nivel extra de rigor para incluso aquellas relaciones y transacciones no detectadas, tal vez deberían analizarse enfoques alternativos para esos elementos. El muestreo estadístico y la verificación regular de detecciones de los elementos excluidos son maneras adecuadas de validar el proceso de decisión basado en el riesgo del departamento de cumplimiento y de los controles de su programa. ¿Por qué no elegir un día al azar y buscar a aquellos nombres birmanos molestos en una base de datos post-mortem, para satisfacer a la gerencia, auditores y reguladores de que el actual nivel de riesgo involucrado no ha cambiado materialmente? Mensualmente, se puede hacer una revisión exhaustiva de un subconjunto de cuentas de clientes excluido contra las fuentes de noticias adversas en los medios podría producir un informe que podría ser analizado más eficientemente que utilizando un sistema en línea de administración de casos, especialmente cuando se asume la inocencia, y solo las excepciones necesitan una acción afirmativa.

Vale destacar que, a pesar de los mejores esfuerzos, la posibilidad de que las señales de alerta más evidentes sean justiciables es baja. El truco es saber cuándo un evento desapercibido pasa a tener una importancia que puede ser ignorada y cuándo requiere nuestra atención.

El cumplimiento sin tener en cuenta los costos es insostenible; coloca a las compañías en una desventaja competitiva. Sin embargo, el incumplimiento sin tener en cuenta los costos también es poco prudente; las respuestas regulatorias pueden dificultar seriamente la habilidad de la empresa para realizar su negocio.

Lo que se necesita es una evaluación clara de los riesgos regulatorios e, igual de importante, las posibles respuestas regulatorias. Asumiendo la respuesta más severa, o la más benigna, ambas valuarán incorrectamente el precio del riesgo, lo que generará una inversión inadecuada de los esfuerzos de cumplimiento. De esa manera, podemos concentrarnos en cumplir las regulaciones de maneras que puedan tener un impacto material en los estados de ganancias y pérdidas de nuestras empresas y enfocarnos menos en aquellos que tengan muchas menos probabilidades de tener ese impacto.

Eric A. Sohn, CAMS, senior engagement manager, Accuity, Skokie, IL, EE.UU., eric.sohn@accuitysolutions.com engagement manager, Accuity, Skokie, IL, USA, eric.sohn@accuitysolutions.com

Lavado de dinero: un personaje central en un thriller financiero, Clearing House (Casa de Compensación)

Clearing House por Michael Lee Cannon

La banca corresponsal es considerada una tipología de alto riesgo de lavado de dinero por el Grupo de Acción Financiera Internacional (GAFI) por varias razones, incluido el hecho de las astronómicas sumas de dinero que pueden provenir de muchas direcciones y la banca corresponsal ofrece servicios a clientes indirectos, p.e., individuos y entidades cuyas identidades nunca han sido verificadas ni para quienes se ha obtenido conocimiento de primera mano.

En *Clearing House*, el autor Michael Cannon escribe un cuento de banca corresponsal utilizada para lavar enormes sumas de dinero en todo el mundo. El personal principal comienza como un lavador de bajo nivel en una organización criminal, pero después de pasar un gran susto con una pandilla competidora, decide que necesita cambiar su actividad. Obtiene el título de abogado (pagado por la organización criminal), y se convierte en un respetable hombre de negocios en el mundo financiero de Nueva York dirigiendo un negocio de servicios monetarios (NSM) muy progresista que presta servicios a las poblaciones inmigrantes en las principales ciudades de los EE.UU. — mientras que al mismo tiempo ayuda al sindicato del crimen organizado a lavar millones en todo el mundo. Establece su reputación no solo como un hombre de negocios inteligente y exitoso, pero como un cierto dechado de virtudes por prestar servicios bancarios a aquellos que son ignorados por los bancos tradicionales, en gran parte, las clases más bajas.

Escrita como una historia de suspenso, el señor Cannon combina de manera efectiva muchos temas y situaciones en una historia ficticia — de mucho suspenso ya que es muy creíble, especialmente si el lector resulta ser un profesional de cumplimiento. Al leerla, resulta muy convincente y uno puede aceptar rápidamente que todas las situaciones podrían ocurrir realmente.

La historia incluye varias posibles situaciones ALD. El protagonista, Jorge, comienza fundando un NSM, el cual amplía para usar contactos no solo en la industria del juego, sino también en otros negocios para facilitar el lavado de dinero. También tiene contactos dentro de la Reserva Federal de Nueva York, que lo mantiene informado de los acontecimientos regulatorios. Para aumentar la percepción de la integridad del NSM, Jorge contrata oficiales de cumplimiento de los bancos más prestigiosos del área de la ciudad de Nueva York.

El NSM es identificado como un potencial cliente de servicios de transacción/pago por una sucursal de uno de los bancos más prestigiosos de la ciudad de Nueva York. Cuando se le pide al banquero encargado de hacer transacciones que presente una propuesta para ofrecer servicios de banca corresponsal, su reticencia inicial se convierte en una buena relación de trabajo con Jorge. Después de pedir su opinión y consejo sobre cómo aumentar su negocio, Jorge comienza a buscarlo para ofrecerle ser empleado. Finalmente contrato al banquero de transacciones y básicamente le da una carta blanca para aumentar el negocio a través del banco, lo cual hace con enorme éxito. Cuando surge la necesidad de lavar grandes sumas de dinero, empieza a hacer contactos para establecer una red global de corresponsalía.

Una de las primeras relaciones que surge es con un conocido del dueño de un NSM, que es ejecutivo de un banco en Miami. Este banco es utilizado como corresponsal para sus negocios latinoamericanos, que se agranda después de los viajes del banquero a las principales ciudades de Latinoamérica y Sudamérica. Continúa tratando de ampliar su red viajando a varias ciudades en todo el mundo, conversando con posibles bancos corresponsales.

El castillo de naipes empieza a derrumbarse cuando otra investigación, esta vez de pagos desde un hawalader pakistaní lleva a los investigadores federales estadounidenses a la oficina central del NSM, pidiendo detalles de los pagos realizados. El banquero de transacciones hace más preguntas, cuando comienza a cuestionar los enormes e impredecibles incrementos del negocio a las oficinas móviles, cuyo concepto había propuesto en primer lugar. A medida que los reguladores solicitan información adicional sobre las transacciones para rastrear los pagos hechos por el hawalader, el personal de cumplimiento recibe la instrucción de cooperar totalmente con las autoridades. Los resultados de éstas conllevar a amenazar con descubrir a Jorge.

Uno de los temas presentes en todo el libro es el plan de contingencia de Jorge. Desde su época de lavador, o pitufo, siempre tenía varios planes alternativos para protegerse. Esta situación subsiste hasta el momento culminante del libro.

Si bien el libro podría tener una mejor redacción (lo que estoy seguro ocurrirá en la próxima edición), es uno de esos libros que *"uno no puede parar de leer"*. Yo recomiendo mucho el libro a todos aquellos que actúan en el campo ALD y/o la banca corresponsal. ¡Les hará pensar mucho y los sorprenderá hasta hacerlos asustarse!

http://michaelleecannon.com/

Escrito por Carolyn E. Vick, CAMS, ED, Global KYC Strategy manager, TS Sales KYC/ Compliance, JPMorgan Chase, Nueva York, NY, EE.UU., carolyn.e.vick@jpmchase.com

Compartir la riqueza del conocimiento

Pregúnteles a cualquiera de mis hermanos sobre mi trabajo y la respuesta será "ella trabaja en un banco". Mi carrera bancaria se ha extendido durante casi tres décadas y me ha llevado desde banca en sucursales a operaciones de préstamos a los consumidores, desde relaciones con clientes ejecutivos hasta cumplimiento general y cumplimiento antilavado de dinero (ALD).

No hablo mucho sobre mi trabajo — incluso con mis amigos. Parte de la información que interpreto, divulgo y de alguna manera "manejo" produce mucho miedo — como el financiamiento del terrorismo y el predominio del tráfico humano. A nivel personal, los dos temas son intimidatorios por sí mismos pero cuando se le agrega el conocimiento de que está sucediendo dentro del propio país, el conocimiento adquiere otras dimensiones mayores. Para aquellos de nosotros que han tenido la fortuna de trabajar en la vigilancia ALD, ¡sabemos que el trabajo puede ser apasionante y monótono muy a menudo al mismo tiempo! Sin embargo, los profesionales ALD son los embajadores perfectos del intercambio de información conocida en el trabajo, los webseminarios y los seminarios para conocer a expertos de la industria.

Llamado a la acción

Hay muchas maneras en las que los profesionales ALD pueden intercambiar conocimientos para beneficio de sus familias, amigos y sociedades. Una conversación casual en una cena con familia y amigos es el lugar perfecto para hablar de su trabajo. Sin dudas que alguna parte de la información es privada, por lo que hay que saber distinguir muy bien qué información se elige compartir. Sin embargo, mucha de la información sobre fraude, estafas y esquemas es pública — pero el público (incluidos nuestros amigos y familia) no tienen el tiempo o la inclinación para buscar los conocimientos. Los profesionales ALD tienen la oportunidad de dar sus conocimientos a sus conocidos en una bandeja de plata.

Los profesionales ALD tienen la oportunidad de dar sus conocimientos a sus conocidos en una bandeja de plata

Pocos fuera del área ALD podrían reconocer un esquema de Anticipo de Honorario *(Advance Fee scheme)*[1] o un esquema Ponzi[2], lo que hace que posteriormente muchas personas caen víctimas de estos esquemas todos los años. Muchos profesionales ALD pueden definir, de memoria, los indicadores de estos esquemas. Y aquellos profesionales ALD que no pueden recitar las definiciones, por lo menos saben dónde buscar la información. Los profesionales ALD deberían analizar las "señales de alerta" de esto esquemas durante una cena familiar. Hacerles saber a la gente que quieren que uno está a disposición para discutir cualquier posible tema vinculado a inversiones no convencionales o mensajes de correo electrónica que hayan recibido de desconocidos. Hablar con ellos sobre las estafas con loterías,[3] las estafas 419,[4] el *phishing* y el *pharming*, y cualquier otra estafa, esquema y fraude que uno pueda conocer. Explicar que las solicitudes de dinero por anticipado de un extraño (y a veces incluso de conocidos — piensen en el "fraude por afinidad[5]") por un pago posterior inusualmente grande es una señal de alerta de numerosas estafas (Nigeriana, Lotería, Ponzi etc.).

Grandes fuentes

Si alguno de nuestros familiares no se siente cómodo dando información financiera, hay que alentar a nuestros seres queridos a que busquen información en sitios imparciales como la Comisión Federal de Comercio (*Federal Trade Commission*, o FTC, por sus siglas en inglés). La FTC es solo una de las agencias gubernamentales que educa a los consumidores sobre las prácticas injustas y engañosas.[6] La oficina del Inspector Postal[7] también considera que si cuentan con el conocimiento adecuado, las potenciales víctimas pueden defenderse contra las tácticas de venta agresiva. Otro recurso excelente sobre la prevención de esquemas de estafas y fraudes actuales es la sección de recursos sobre fraudes del sitio web de la Oficina de Contralor de la Moneda (Office of the Comptroller of the Currency).[8]

En lugar de enviar una cadena de mensajes de correo electrónico que nadie quiere leer realmente, envíeles a sus amigos y familiares un email que realmente apreciarán, dedicado a proteger sus identidades, bienes y/o futuro. Elija un "tema candente" como un esquema Ponzi de alto perfil y desglóselo en elementos llevados a la práctica para sus amigos y familiares. Si correspondiere, identifique áreas donde la víctima podría ser más diligente al realizar investigaciones sobre los antecedentes. O, identifique algunos sitios que sean de fácil utilización con información interesante dedicada a la protección del consumidor. Tanto FinCEN como el IRS tienen casos de estudio en sus sitios en Internet que son interesantes e informativos — incluso para aquellos que están fuera del mundo ALD/fraude. Los sitios indicados son solo dos de los cientos de sitios a disposición para armar al ciudadano común con conocimientos para protegerse de los estafadores y defraudadores. Tómese el tiempo para establecer qué sitios serían de mayor beneficio para sus destinatarios, el abrumarlos con información podría hacer que no lean cualquier información importante incluida en el email.

Sea la fuente

A medida que educa a su familia y amigos, piense en otras áreas en la comunidad que podrían beneficiarse con sus conocimientos. Las escuelas y las organizaciones que atienden a las personas mayores estarán, en la mayoría de los casos, ansiosas por aceptar su solicitud para hablar ante ellas. Las escuelas elementales tienen clases de Junior Achievement (*Logros de Jóvenes*), las escuelas medias tienen programas de días de carreras profesionales y las escuelas secundarias ofrecen clases de negocios y economía. Las organizaciones que atienden a las personas mayores a menudo auspician clases de educación y cursos sobre administración del dinero. Sea cuidadoso y limite las discusiones sobre las señales de alerta y los esquemas que hay que evitar. No caiga en la trampa de recomendar determinadas inversiones o tipos de inversiones a menos que sea un asesor de inversiones autorizado.

Además, fíjese la protección que su institución financiera puede brindarle a sus clientes y las comunidades. Considere la posibilidad de entrenar a los asociados de las sucursales bancarias sobre las señales de alerta de los esquemas con anticipos de honorarios y el abuso de personas mayores. El personal de la oficina de apoyo, incluidos los procesadores de cheques, podrían ser entrenados para cuestionar transacciones importantes fuera de lo común. No es necesario decirlo, el personal ALD y de Fraude también podría ser capacitado sobre las señales de alerta de fraude y otras actividades ilegales. Los defraudadores son astutos y están constantemente perfeccionando su oficio. Los profesionales ALD y de fraude deben permanecer vigilantes para poder detectar las señales de distintos tipos de fraude (hipotecario, tarjetas de crédito, cheques sin fondos, etc.) Considere la posibilidad de hacer que su organización financiera organice una sesión de capacitación después del horario de trabajo. Además de brindar un servicio muy necesario a la comunidad, es una gran oportunidad para conseguir nuevos clientes y cumplir con las expectativas de la Ley de Reinversión en la Comunidad (*Community Re-investment Act*, o CRA, por sus siglas en inglés).[9]

¿Víctimas típicas?

Al realizar la investigación para este artículo, me sorprendió saber que muchos de los estereotipos de las víctimas de fraude son incorrectos. A continuación de detalla un cuestionario rápido para poner a prueba su conocimiento sobre el fraude y las víctimas de fraude:

1. La víctima típica de fraude por telemercadeo es:
   a. Una persona mayor
   b. Tiene dificultades financieras
   c. Tiene nivel de educación de escuela secundaria

2. El fraude típico tiene menos posibilidad de tener éxito cuando:
   a. El defraudador tiene menos de 50 años de edad
   b. El contacto inicial es por teléfono o correo electrónico
   c. La "inversión" es de US$100.000 o más

[1] http://www.secretservice.gov/faq.shtml#faq13
[2] Diciembre 2009 ACAMS Today-Más Allás de los Titulares: La posición de Un Investigador sobre los esquemas Ponzi
[3] http://www.consumerfraudreporting.org/lotteries.php
[4] http://home.rica.net/alphae/419coal/
[5] http://www.sec.gov/investor/pubs/affinity.htm
[6] http://www.ftc.gov/reports/fraud97/cons-ed.htm
[7] https://postalinspectors.uspis.gov/
[8] http://www.occ.treas.gov/topics/consumer-protection/fraud-resources/index-fraud-resources.html
[9] http://www.fdic.gov/news/news/financial/2007/fil07006a.html

3. Una encuesta realizada en 1992 sobre fraude por telemercadeo encontró que uno de cada tres estadounidenses informó haber sido engañado y perdido dinero mediante varios medios engañosos. ¿Cuántas víctimas reportaron el delito?
   a. Menos de un tercio
   b. Dos tercios
   c. 90%

Verifique sus respuestas:

Respuestas:

1. a — Una persona mayor. Las personas mayores son buscadas específicamente por las personas que hacen telemercadeo porque es más probable que se mantengan en línea escuchando los anuncios de la venta agresiva[10] y "tienen una mayor concentración de riqueza que el público en general.[11]

2. b — El fraude típico tiene menos posibilidades de prosperar si el contacto inicial es por teléfono o mail. Las víctimas que hacen un *contacto personal* con los defraudadores tienen más probabilidades de confiar en obtener un resultado positivo.[12]

3. a — Menos de un tercio de los estadounidenses reportaron haber sido engañados mediante fraude con telemercadeo en una encuesta de 1992. Incluso más alarmante, es el hecho de que solo un tercio de las personas encuestadas (víctimas y no víctimas) considera que sabe cómo determinar si una oferta es legítima, lo que subraya aún más la necesidad de que aquellos de nosotros que estamos al tanto de la información sobre educación financiera la compartamos con familiares, amigos, escuelas y clientes.

Inevitablemente, los defraudadores se aprovechan de los vulnerables. El abuso de personas mayores[13] está recibiendo mucha atención de la prensa recientemente — mucha de la cual se concentra en el aprovechamiento financiero de las personas mayores. Cuando los defraudadores se aprovechan de una persona de edad, además de cometer delitos de fraude y lavado de dinero, también cometen el delito de abuso de personas mayores. El Centro Nacional sobre Abuso de Personas Mayores (*National Center on Elder Abuse*, o NCEA, por sus siglas en inglés)[14] define al abuso de personas mayores como *"cualquier acto a sabiendas, intencional o negligente realizado por un cuidador o cualquier otra persona que cause un daño o un riesgo serio de daño a un adulto vulnerable"*. El NCEA delega en las leyes y regulaciones estatales la definición de violaciones específicas de las personas de edad.

En febrero de 2011, FinCEN publicó una guía para las instituciones financieras sujetas a Reporte de Operaciones Sospechosas (ROS) para incluir el término "explotación financiera de una persona mayor" en la descripción cuando se reporta una sospecha de abuso de una persona mayor. Esto incluía al fraude financiero y subrayaba que la posible victima no debe ser identificada como sospechosa en el formulario del ROS sino que la información sobre la víctima debería ser incluida en el capítulo Parte V (la descripción).[15]

Recientemente, la Ley Dodd-Frank de Reforma de Wall Street y de Protección al Consumidor dio el audaz paso de codificar la definición de vulnerable. "Las personas mayores, las personas que enfrentan barreras de idio, las personas de bajos ingresos y las minorías"[16] se encuentran entre los grupos identificados específicamente como "vulnerables" bajo el Título XIV de la Ley Dodd-Frank Title — Reforma Hipotecaria y Préstamos Anti-Depredadores.

Fraude + ALD = FRALD

Usted puede estar pensando internamente, ¿por qué estoy leyendo esto en una revista especializada en ALD? La respuesta a esa pregunta está en realidad compuesta de varias razones. Primero, analicemos el Reporte de Operación Sospechosa de FinCEN (ROS). La Parte III del formulario de ROS[17] incluye una lista de varios fraudes como delitos subyacentes de lavado de dinero (p.e., fraude con tarjetas de crédito, fraude hipotecario, fraude con prestamos al consumidor y comerciales). Pensando lógicamente, los defraudadores están en la actividad de fraude por el dinero, más específicamente, por la ganancia. Para disfrutar completamente de los beneficios obtenidos ilegalmente con la estafa/fraude, el defraudador colocará los fondos, de alguna manera, en el sistema financiero. ¿Suena un poco a la colocación, no es así?

Segundo, como el gurú del ALD John Byrne escribió en un artículo redactado junto con Chris Swecker recomendando la convergencia de los programas ALD y antifraude de las instituciones financieras, "Los criminales financieros no operan en divisiones separadas, como las grandes instituciones financieras han organizado típicamente sus programas ALD y de prevención del fraude. Los profesionales ALD tienen una necesidad inherente de entender al fraude y los profesionales del fraude ciertamente se beneficiarán al conocer el ALD. Seguir el ritmo del mundo externo a través de la convergencia de los programas de fraude y ALD dentro de las instituciones financieras reducirá los riesgos y costos y ayudará a las organizaciones a seguir el ritmo de las amenazas que pueden estar enfrentando".[18]

Tercero, una forma segura de disminuir la incidencia del lavado de dinero como resultado de los esquemas fraudulentos es limitar la cantidad de posibles víctimas. Cuanta más gente sepa, más podrán evitar caer víctimas de estos actos. Sin víctimas, el fraude fracasa. Es así de simple.

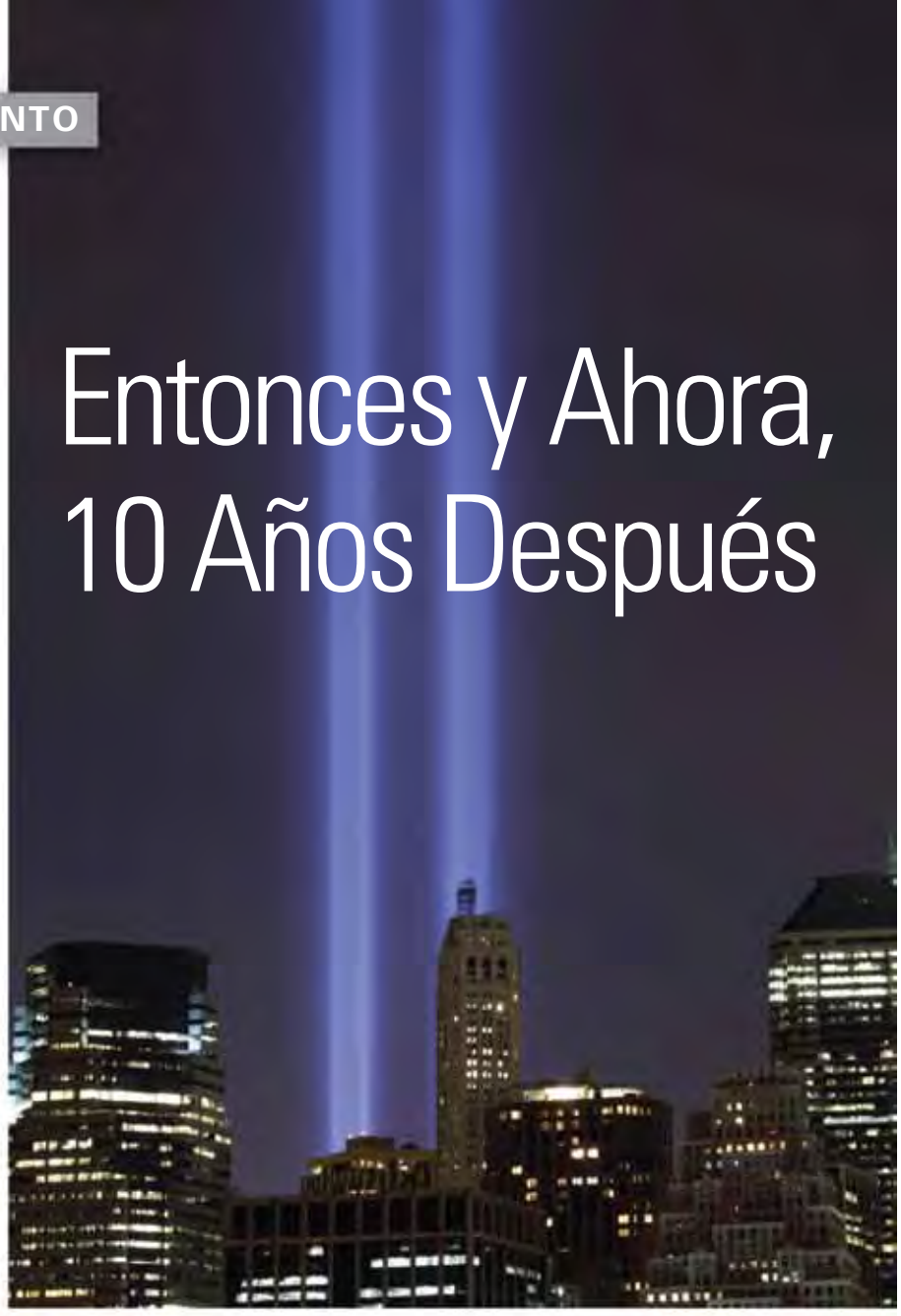
Aunque puede haber ciertas áreas donde los programas contra el fraude y ALD difieran, la educación de público de diversas maneras para evitar que sean víctimas del fraude no debería ser una sola. Todos necesitamos compartir la información valiosa que tenemos sobre el fraude y las estafas, sea en casa, el trabajo o la comunidad. Los profesionales ALD y de fraude deberían ser alentados a luchar contra el fraude/ALD en la primera línea mientras continuamos haciendo nuestro trabajo en la parte trasera. En algún punto, el conocimiento que compartan salvará el dinero de alguien y hará que un defraudador estafe a una víctima menos. ¡Realmente no hay nada mejor que eso!

Amy Wotapka, CRCM, CAMS, CFE, CIPP, FCRA, ASQ CQIA, requirements manager Corporate Compliance, Capital One, Richmond, VA, EE.UU., amy.wotapka@capitalone.com

[10] http://www.occ.treas.gov/topics/consumer-protection/fraud-resources/index-fraud-resources.html
[11] http://www.fincen.gov/statutes_regs/guidance/html/fin-2011-a003.html
[12] http://www.popcenter.org/library/crimeprevention/volume_12/08-Titus.pdf
[13] http://www.fincen.gov/news_room/nr/html/20110218.html
[14] http://www.ncea.aoa.gov/NCEAroot/Main_Site/About/What_We_Do.aspx
[15] http://www.fincen.gov/statutes_regs/guidance/html/fin-2011-a003.html
[16] Dodd-Frank Sec. 1443 a(4)(A)
[17] http://www.fincen.gov/forms/files/f9022-47_sar-di.pdf
[18] http://www.ababj.com/briefing/tear-down-those-walls-bring-together-aml-bsa-now-2.html

11/9...

Entonces y Ahora, 10 Años Después



Hay pocos eventos en la vida que evoquen una emoción profundamente arraigada y un recuerdo vívido. Los ataques terroristas contra los Estados Unidos cometidos por Al Qaeda el 11 de septiembre de 2001 son claramente uno de esos momentos históricos que permanecen congelados en nuestras mentes. Recuerdo patéticamente mi reacción personal entonces y cómo me afecta ahora. El 11/9 cambió mi vida, como la vida de muchos de nosotros. Yo estaba agobiado con una sensación de querer responder directamente a esos ataques inadmisibles. Afortunadamente, como agente a cargo del Programa de Crímenes Financieros del FBI, estuve en una situación única donde tuve la oportunidad de responder de una manera que muy poca gente pudo. Estuve en una posición para "seguir el dinero". En retrospectiva, ése fue el lugar más gratificante para estar.

Uno de los primeros lugares a los que me dediqué fue el sector de servicios financieros (SSF). Nuestras instituciones financieras son un depósito de huellas digitales financieras que las autoridades de control legal pueden utilizar para seguir al dinero. Las finanzas y las comunicaciones son las dos vulnerabilidades más grandes de las organizaciones para los criminales y terroristas. La habilidad para seguir el dinero para identificar y desbaratar la actividad terrorista es un arma poderosa. La respuesta que tuvimos del SFF fue extraordinaria. Estoy muy orgulloso por cómo respondió la industria, movilizada por un sentido de patriotismo, deber y compromiso. En los días, meses y primeros años que siguieron al 11/9, el FBI y los segmentos del SSF trabajaron en equipo para establecer cinco iniciativas diferentes para investigar proactivamente el financiamiento del terrorismo. Tuve el privilegio de participar directamente en estas iniciativas y fui testigo de primera mano de la dedicación de nuestros socios del sector privado. Además del FBI y otras agencias federales, estas iniciativas incluyeron:

- Un grupo de trabajo de representantes de aproximadamente 20 instituciones financieras. Este grupo estaba formado por oficiales de cumplimiento antilavado de dinero (ALD) y de investigaciones de fraude. Este grupo se concentró en cómo los bancos podían brindar información financiera a las autoridades de control legal de una manera más oportuna y eficiente.
- Algunos proveedores selectos de servicios financieros estaban en posición de prestar legalmente servicios de control legal con información sobre transacciones casi en tiempo real a los fines de las investigaciones.
- Una red de contactos específicos funcionaba 24/7 en más de 200 instituciones financieras. Un representante designado por el banco estaba a disposición permanentemente para brindar información a las autoridades de control legal sobre las pistas de amenazas terroristas.
- Un proveedor de servicios financieros creó una plataforma para que las autoridades de control legal obtuvieran legalmente cierta información específica sobre las transacciones. Esta información no solamente era de fundamental importancia para las investigaciones locales, sino que también le permitió al FBI entregar información financiera a otro país que colaboraba con un servicio de inteligencia para impedir seis ataques terroristas en ese país.
- Un grupo de trabajo de representantes de siete importantes instituciones financieras. Este grupo trabajó en temas sensibles de alto nivel cuyo objetivo era

mejorar el intercambio de información entre las autoridades de control legal y las instituciones financieras.

Mucha gente que trabajaba en el SFF contribuyó a las iniciativas mencionadas y fueron verdaderos héroes olvidados. Su trabajo incansable y generoso detrás de la escena le permitió a las autoridades de control legal tener éxito una y otra vez. Desafortunadamente, la mayoría de ellos no era consciente de lo importante que fueron sus colaboraciones y aún siguen siéndolo. Estas iniciativas de colaboración sirvieron como modelo para las asociaciones pública y privada. Esas asociaciones son esenciales para nuestra habilidad para realizar investigaciones significativas e impedir las actividades terroristas.

A través del correspondiente proceso legal, el Departamento del Tesoro de los EE.UU. obtuvo información de los mensajes de SWIFT de manera reiterada. El FBI fue el consumidor final de esta información que fue utilizada sobre una base limitada, subyacente y dirigida a un objetivo específico. Esta iniciativa fue extremadamente sensible y una importante herramienta de investigación.

Entonces, ¿dónde estamos como país y como industria 10 años después?

Actualmente, nosotros como país estamos mucho más atentos y estamos mucho más al tanto de nuestra vulnerabilidad ante el terrorismo que lo que estábamos antes del 11/9. De la misma manera, el SFF está más comprometido y determinado para erradicar esas instancias en donde los terroristas explotan a las instituciones financieras en apoyo de las actividades terroristas.

Por el lado del gobierno, hemos dado enormes pasos para avanzar. Al evaluar nuestras capacidades de investigación y obtención de información antes del 11/9, estábamos pésimamente preparados, y lo que es peor, éramos sistemáticamente deficientes. El FBI y la CIA fueron muy criticados. Ambas agencias hicieron cambios destacados a sus culturas institucionales. Lo que hemos visto en los últimos 10 años ha sido una transformación significativa en nuestra capacidad para hacer frente al desafío de enormes proporciones de la amenaza del terrorismo. El gobierno ha logrado enormes beneficios cada vez mayores en las líneas de las agencias para detectar, impedir y prevenir ataques terroristas. Han habido algunos percances ocasionales. Sin embargo, hemos demostrado consistentemente una sofisticación mejorada y la ejecución de estrategias contraterroristas. Nuestras capacidades de investigación, inteligencia, de sanción, diplomáticas y militares han frustrado colectivamente numerosas amenazas terroristas en los últimos 10 años. El momento fundamental de esto fue la muerte de Osama Bin Laden por parte de los Navy Seals el 2 de mayo de 2011. La coordinación, cooperación y comunicación entre la CIA y los Navy Seals fue un momento definitorio y resultó en una de las mayores operaciones de inteligencias que hemos realizado como país.

Por el lado del sector privado, especialmente en el SFF, el desafío ha sido diferente aunque silenciosamente exitoso. Como se indicara anteriormente, el FBI ha participado en una serie de iniciativas públicas-privadas productivas relacionadas con el financiamiento del terrorismo. Otras agencias federales han tenido colaboraciones exitosas entre sí y con el sector privado.

> Las instituciones financieras son la línea frontal de nuestra lucha contra el terrorismo

Además, el sector privado, con grandes esfuerzos, ha creado grupos de trabajo cohesivos y dedicados que han contribuido con las iniciativas gubernamentales relacionadas con el financiamiento del terrorismo. Las instituciones financieras son la línea frontal de nuestra lucha contra el terrorismo. Los terroristas inevitablemente utilizan canales financieros formales o informales para movilizar y tener dinero disponible cuando lo necesiten. El uso por parte de los terroristas de las instituciones financieras como una herramienta de facilitación para movilizar el dinero y acceder a él convierte a la función de cumplimiento bancario en un componente esencialmente importante de la seguridad nacional. Es posible identificar a los terroristas y a sus canales de fondeo. Sin embargo, no es probable, o posible, que esto pudiera lograrse sin la participación específica del gobierno. Aún con datos específicos, sería difícil identificar el financiamiento del terrorismo. La posibilidad contra el desafío de la probabilidad es uno de los retos más importantes que enfrentamos. De manera similar al gobierno, a medida que pasaron los años desde el 11/9, el sector privado ha logrado grandes mejoras al tratar con el financiamiento del terrorismo a través del monitoreo de transacciones. Cuanto más puede la industria mejorar la posibilidad de identificar las actividades de financiamiento del terrorismo, más se incrementa la probabilidad de detección de tal actividad. En este aspecto, aún los pasos más pequeños para avanzar en ese sentido pueden ser fundamentales, como se ha demostrado de manera selectiva.

La Ley U.S.A. PATRIOT fue promulgada el 26 de octubre de 2001. Ése fue un momento fundamental en la creación de un marco para combatir al terrorismo de manera efectiva. La Ley PATRIOT les otorgó facultades de investigación a las comunidades de control legal y de inteligencia. Les permitió intercambiar información de inteligencia, lo cual no había sido posible hasta entonces. Ésta era una de las deficiencias más importantes en nuestra situación previa al 11/9. La Ley PATRIOT también trajo regulaciones nuevas y reforzadas para las instituciones financieras. Las obligaciones ampliadas de reporte establecidas por la Ley de Secreto Bancario fueron costosas y gravosas en cuanto a la carga de tareas para las instituciones financieras. No obstante ello, el SSF respondió e implementó programas antilavado de dinero sólidos que en última instancia beneficiaron al control legal y la lucha contra el financiamiento del terrorismo. Soy un firme convencido de que los beneficios para el control legal y los niveles reforzados de diligencia debida tomados por los bancos han sido mayores que las cargas, impidiendo así finalmente el flujo de fondos terroristas.

¿Estamos más seguros hoy que lo que estábamos el 11/9?

Por una variedad de razones, estamos mucho más seguros hoy que lo que estábamos el 11/9.

- Primero y más importante, nosotros como nación no consideramos a nuestra seguridad como algo por sentado o seguro, como hacíamos antes del 11/9. Sabemos que somos vulnerables a un ataque terrorista. Como sociedad, esto nos convirtió en una nación extremadamente alerta. Esta vigilancia ha resultado en al menos dos casos, el último año, donde el público reportó actividades sospechosas que

resultaron en los arrestos de individuos que tenían intenciones de cometer actos terroristas.

- Las comunidades de control legal y de inteligencia han mejorado enormemente sus capacidades humana y de indicadores de inteligencia. Antes del 11/9, ésta era una deficiencia significativa. La inteligencia reforzada ha resultado en la prevención de varios ataques terroristas desde el 11/9.
- El control legal ha sido más proactivo y agresivo al utilizar técnicas sofisticadas de investigación para identificar y prevenir ataques terroristas.
- La utilización por parte de la CIA de misiles drone para apuntar y matar al liderazgo de Al-Qaeda esencialmente ha reducido y neutralizado lo más importante del grupo Al-Qaeda.
- Las acciones militares, diplomáticas y las sanciones han erosionado más la habilidad de los terroristas para funcionar y para tener la capacidad de la organización para atacar a nuestra nación.
- La explotación de la información financiera basada en la colaboración entre las autoridades de control legal, el Departamento del Tesoro y el SSF ha interrumpido los flujos de fondos terroristas y les ha permitido a las autoridades de control legal tomar medidas proactivas de investigación para impedir y prevenir actividades terroristas.

Desafortunadamente, aún cuando estamos mucho más seguros que lo que estábamos el 11/9, probablemente vaya a haber otro ataque en los Estados Unidos. Somos una sociedad abierta y por lo tanto vulnerable ante los ataques. Sea que el ataque sea en la escala del ataque del 11/9 en el que participaron aeronaves, o como los ataques en Madrid y Londres, realizados en los sistemas de tránsito por ferrocarril o subterráneos, o como el ataque de escasa tecnología igualmente mortal y atroz como el ocurrido en Bombay o como los ataques en los hoteles en Pakistán, Jordania y Afganistán, va a ocurrir un ataque. Hemos sido sacudidos por un puñado de ataques como el de Fort Hood, el ataque cometido en Noruega el 22 de julio de 2011, cómo un solo atacante solitario puede causar muertes y destrucción masiva. El ataque cometido en Noruega el 22 de julio de 2011, cómo un solo atacante solitario puede causar muertes y destrucción masiva.

Poniendo las cosas en perspectiva, somos una nación mucho más segura. Sin embargo, seguimos siendo vulnerables y nos vamos a enfrentar a un ataque terrorista. Cuando eso ocurra, antes de apresurarnos a juzgar, como somos proclives a hacer, debemos evaluar la situación y entender correctamente el problema y la causa del ataque. Debemos tener presente, la enorme cantidad de posibles ataques que impedimos desde el 11/9. ¿Ese ataque exitoso será el resultado de una situación que fallamos detectar o será el resultado de una falla sistémica, como la que encontramos antes del 11/9? Mi sensación es que será una falla. Debemos pedir responsabilidad pero debemos ejercer moderación en pedir cambios hasta que conozcamos todos los hechos.

¿Qué lecciones hemos aprendido en los últimos 10 años?

Estos últimos 10 años han sido una experiencia de aprendizaje. Las lecciones aprendidas incluyen:

- Debemos estar vigilantes.
- Nosotros, como nación, somos extremadamente vulnerables a los terroristas en términos de ataques terroristas y explotación de nuestro sistema financiero.
- Necesitamos conocer verdaderamente nuestros riesgos y las amenazas que enfrentamos.
- Necesitamos ser proactivos para enfrentar la amenaza del terrorismo.
- Necesitamos tener un sentido de la urgencia y de sensibilidad con el tiempo al tratar con el terrorismo.
- El trabajo en conjunto de los sectores público — privado nos brinda una mayor oportunidad para impedir y prevenir actos terroristas.
- La comunicación, cooperación y coordinación entre las agencias gubernamentales y el sector privados es extremadamente importante.
- Las finanzas y la comunicación son las mayores vulnerabilidades de los terroristas.
- Los sectores público y privado deben continuar implementado mecanismos nuevos e innovadores para explotar las vulnerabilidades de los terroristas.
- El seguimiento del dinero y interrupción de los flujos de fondos disminuyen la capacidad de los terroristas de operar o triunfar en sus planes para cometer actos de terrorismo.

Conclusión

El hecho es que, aunque somos extremadamente vulnerables a otro ataque terrorista importante, somos una nación mucho más segura hoy que lo que éramos en la mañana del 11/9. Tenemos mucho por lo que debemos estar agradecidos. A los servidores públicos que nos protegen a diario y trabajan para impedir que los terroristas nos ataquen les debemos nuestra gratitud y respeto. De la misma manera, la enorme cantidad de profesionales de cumplimiento del sector financiero que monitorean y reportan actividades sospechosas y que protegen a nuestras instituciones financieras merecen el reconocimiento. Ellos son nuestros héroes no reconocidos, y necesitan saber esto. Lo que mucha gente no se da cuenta es que el reporte de la Ley de Secreto Bancario, especialmente en la forma del reporte de actividad sospechosa, es increíblemente importante y hace una diferencia significativa.

Aún cuando estamos a diez años de distancia del 11/9, recuerdo vívidamente los eventos que ocurrieron ese día. Nunca olvidaré el sentido de impotencia que sentí o la alegría que experimenté cuando me dí cuenta de la oportunidad que teníamos para "seguir el dinero" e identificar a los atroces individuos responsables del ataque. Esa hazaña se logró en materia de semanas mediante el análisis de registros financieros por parte de las autoridades de control legal, facilitados por el SSF. Esto también crea el escenario para anhelar y crear metodologías para interrumpir el financiamiento del terrorismo. Hay mucho que podemos hacer para impedir la amenaza del terrorismo. Perseguir las balas y las bombas es más sensacional. Sin embargo, la ruta más directa y productiva es seguir a los dólares. La clave es "seguir al dinero". Debemos continuar avanzando y elaborar mecanismos para hacer que les sea más difícil y desafiante a los terroristas poder usar nuestro sistema financiero. La clave es entender el flujo y tomar los posible y hacerlo probable.

Dennis Lormel, presidente & CEO, DML Associates, LLC, Lansdowne, Virginia, EE.UU., dlormel@dmlassociatesllc.com

Asociación de Especialistas Certificados en Antilavado de Dinero
ACAMS

aldlatinoamerica.org

5ta Conferencia Anual Latinoamericana sobre Lavado de Dinero de ACAMS

9 al 11 de noviembre del 2011 ■ JW Marriott Cancún ■ México





AHORRE US$50
Inscríbase y pague antes del 14 de octubre. Mencione el código **AT-50**

Capacitación antilavado para todas las industrias, sectores e instituciones

- **APRENDA** las mejores prácticas, soluciones y lecciones de casos reales domésticos e internacionales
- **ACTUALÍCESE** sobre las nuevas tendencias y tipologías de lavado de dinero y otros delitos financieros
- **ENTIENDA** los recientes e importantísimos desafíos legales de EE.UU. que afectarán a su organización
- **FORTALEZCA** su carrera y crezca profesionalmente con el mejor conocimiento de los líderes de la industria

¡INSCRÍBASE AHORA! aldlatinoamerica.org ■ +1 786.871.3068 ■ sleon@acams.org

PATROCINADORES DIAMANTES

Salles Sainz Grant Thornton

WORLD-CHECK™ A THOMSON REUTERS BUSINESS

PATROCINADOR PLATINO

world compliance

PUBLICACIÓN PATROCINADORA

Lavadodinero.com

Diligencia debida sobre el cliente: ¿Costo regulatorio o principio básico de un buen negocio?

La diligencia debida sobre el cliente (DDC) es el principio básico de todos los programas LSB, ALD, un principio fundamental de la 3er. Directiva sobre Lavado de Dinero de la Unión Europea, y una obligación común en todos los regímenes ALD, sin importar su ubicación geográfica. En el último año, el foco de atención regulatorio sobre la DDC ha aumentado considerablemente. Como con la mayoría de las áreas que se encuentran bajo la atención regulatoria, tenemos más posibilidades de ver discusiones sobre la implementación deficiente del programa como parte de los procedimientos de control legal, que un análisis sobre cómo los programas DDC bien implementados pueden llevar a importantes beneficios comerciales tanto dentro como fuera de los equipos de cumplimiento.

En el corazón de la DDC están los principios fundamentales del conocer al cliente, definiendo el contexto en el cual es aceptable hacer negocios con un cliente, y conocer los fundamentos sobre los cuales se desarrolla constantemente la relación con el cliente. Los principios de la DDC son simples e históricamente han sido un requisito clave de la buena práctica bancaria — donde los

clientes son conocidos, las interacciones comerciales son entendidas y las relaciones comerciales crecen dentro de una red bien controlada de confianza y conocimiento. Dado este contexto, ¿por qué entonces la DDC es considerada por algunas empresas una carga regulatoria ALD onerosa y no una función fundamental, base principal de cualquier negocio exitoso?

En este artículo analizamos las estrategias para una DDC exitosa, cómo pueden obtenerse beneficios de los programas DDC, cómo los procesos DDC pueden ser aplicados más ampliamente a otras áreas comerciales, y cómo las mejores prácticas en la DDC generan beneficios en todo el programa ALD de una institución.

Guía regulatoria

Tenemos bastantes regulaciones y guías regulatorias asociadas con la DDC. Por ejemplo, ocho de las 40 Recomendaciones del GAFI se relacionan directamente con la diligencia debida sobre el cliente, con recomendaciones clave para las instituciones comerciales y corresponsales. Además, el recientemente reorganizado Capítulo X del Código de FinCEN de Regulaciones Federales, Título 31 CFR 1010.220, se refiere a las obligaciones de identificación del cliente, el Título 31 CFR 1010.610 detallas los requisitos aplicables a la banca corresponsal, y el Título 31 CFR 1010.620 fija las obligaciones para la banca privada. La DDC también es objeto del Capítulo 2 de la 3er. Directiva sobre Lavado de Dinero de la Unión Europea; el Banco Internacional de Pagos ofrece su propia guía asociada con el CSC para el ingreso de nuevos clientes, y la JMLSG del Reino Unido establece guías específicas adicionales sobre la DDC.

Dos publicaciones recientes han analizados las diversas complejidades asociadas con la DDC. En mayo de 2011 la Revisión de Actividad de ROS de FinCEN contenía una evaluación de las ventajas de los programas DDC efectivos, con una atención importante en los desafíos asociados con la identificación de las personas expuestas políticamente (figuras políticas extranjeras senior actuales o anteriores, sus familias y sus asociados), un dolor de cabeza para la mayoría de las instituciones. El informe también tenía en cuenta el impacto asociado con la corrupción extranjera, un área de relevancia significativa dados los eventos de la primavera árabe — Túnez, Egipto, Libia y Siria.

Siguiendo con estos temas, en junio de 2011 la Autoridad de Servicios Financieros del Reino Unido (FSA, por sus siglas en inglés) publicó su informe sobre "Administración por Parte de los Bancos de Situaciones de Alto Riesgo de Lavado de Dinero". Este informe contiene los aspectos buenos y malos, y analiza algunos temas sistemáticos asociados con el tratamiento de los clientes de alto riesgo y las PEPs, la aceptación de nuevos clientes, la evaluación del riesgo de los clientes, y las obligaciones de monitoreo reforzados en las relaciones de alto riesgo. El informe destaca que de las firmas analizadas, un tercio manejó inadecuadamente los registros de la debida diligencia, un tercio no identificó correctamente a las PEPs, y un tercio de los bancos visitados no aplicó una DDR significativa. Aunque están focalizados en las compañías del Reino Unido, los resultados destacaron algunos lugares comunes en algunos temas en la práctica en la industria bancaria global.

Requisitos de la debida diligencia sobre el cliente

En el centro de la DDC está el concepto de conocimiento del cliente, aplicado en la apertura de cuenta, al comienzo de la relación comercial, y de manera constante. La diligencia debida simplificada reduce las obligaciones de conocimiento del cliente asociado con determinadas cuentas y clases de clientes pero, en general, la DDC requiere procedimientos manuales o automáticos de identificación del cliente y una ampliación de estos procedimientos para las relaciones comerciales específicas y los dueños beneficiarios comunes en las cuentas comerciales y en las cuentas corresponsales. Las instituciones deben conocer el razonamiento económico de la relación comercial y obtener las características de conducta anticipada del cliente, con la evaluación del riesgo realizada para cada cliente con relación a sus características y a su combinación de productos y servicios.

Para algunas relaciones con clientes selectos, las instituciones financieras deben aplicar procedimientos de debida diligencia reforzada (DDR), por ejemplo, para los clientes de banca privada y los clientes de alto riesgo o aquellos clientes identificados como PEPs. Además, la DDR también es un pre-requisito para los negocios que no son realizados cara a cara y una obligación para muchas instituciones modernas cuyas relaciones con los clientes son llevadas a cabo de manera enteramente remota — p.e., en Internet, por teléfono o, en algunos casos a medida que se desarrolla la tecnología, en todas las plataformas de banca móvil.

Desafíos en la implementación de la DDC

Con el transcurso del tiempo, los ámbitos de los negocios se han vuelto cada vez más complejos — con operaciones multinacionales y varios canales de interacción. Sin embargo, los clientes esperan que los productos y servicios sean entregados de manera consistente, independientemente de dónde y cómo son consumidos estos servicios. A medida que los negocios crecen en tamaño — con relación a la presencia global, la presentación de nuevos productos y servicios, una cantidad cada vez mayor de clientes — las empresas enfrentan varias complejidades en las evaluaciones del riesgo de la DDC, ya que el proceso a menudo es manual, ineficiente, operativamente oneroso y carece de consistencia. A fin de mantener el cumplimiento regulatorio y reducir los impactos negativos sobre el cliente, las empresas deberían analizar formas en las cuales puedan automatizar los procesos manuales de diligencia debida e implementar un enfoque de DDC que permita una mayor agilidad y respuesta al cambio.

Estrategias exitosas de la DDC

Existen tres elementos fundamentales en los programas de DDC exitosos:

- Automatización del proceso
- Evaluación sistemática del riesgo del cliente
- Plataforma común para la investigación y el reporte

La automatización del proceso es fundamental para reducir o eliminar los procesos manuales de aceptación de clientes y de DDC constante. La automatización del proceso debería ser utilizada para automatizar la verificación de la identidad del cliente, monitorear las sanciones y realizar verificaciones sobre las PEPs y las noticias negativas publicadas en los medios. El foco de atención sobre la DDC debería ser dar una respuesta manual solo cuando los riesgos excedan niveles aceptables, donde existan anomalías de la información o donde se requiera el análisis regular del cliente. La automatización del proceso en este nivel reduce el costo de incorporación de clientes nuevos, agiliza el procesamiento y agiliza y mejora la experiencia del cliente. Esto puede mejorar más las eficiencias del costo del proceso e incrementar la competitividad del negocio.

Sin embargo, la automatización efectiva del proceso depende de la evaluación precisa del riesgo del cliente.

Un programa exitoso de DDC requiere que el negocio realice una clasificación y cuantificación del riesgo del cliente. El primer paso en este proceso es una evaluación sistemática de los riesgos del negocio que existen independientemente de las características del cliente, por ejemplo, basándose en el conocimiento de las unidades de negocios y servicios, las ofertas de productos, o las localidades geográficas en donde hay operaciones. En segundo lugar, estos riesgos son trazados con relación a las características y patrones anticipados de uso del producto por parte del cliente. La combinación de la evaluación del riesgo en estos dos niveles permite que los clientes sean agrupados en franjas de riesgo para una mayor evaluación y análisis. Las franjas de bajo riesgo requieren un bajo o nulo escrutinio humano, con mayores niveles de diligencia y frecuencia de análisis requeridos para los clientes ubicados en las franjas de mayor riesgo. Este enfoque de la evaluación del riesgo permite que se apliquen a todos los clientes tratamientos adecuados basados en el riesgo, reduciendo la carga del análisis para los clientes de bajo riesgo y concentrando los recursos de la DDC en aquellos clientes que representen los mayores riesgos comerciales. Este enfoque basado en el riesgo también se alínea con los generadores regulatorios y conduce a eficiencias operativas, tanto para la DDC y también a través de la aplicación de franjas de riesgo como parte del monitoreo de transacciones.

La evaluación del riesgo puede ser realizada interactivamente como parte de la aceptación e incorporación del cliente, con preguntas dinámicas basadas en las características del cliente, los productos y servicios a utilizarse, y el grado de riesgo calculado. Se adaptan formas dinámicas basándose en los requisitos del cliente y el producto, reduciendo la necesidad de que el personal o los clientes completen formularios innecesarios y asegurando que los datos esenciales de la información, documentos y materiales de identificación sean obtenidos correctamente. Además de asegurar la obtención de información precisa, la aplicación correcta de métodos dinámicos de preguntas y respuestas reduce la posibilidad de que la información se filtre con relación a la política de riesgo y minimiza el uso indebido de la información. Esto ayuda a mitigar las inquietudes que surgen asociadas con la manipulación de sistemas por parte de los gerentes de relación y el personal de las sucursales y respalda la evaluación de la idoneidad del cliente respecto de los productos.

Una plataforma de tecnología común, que dé soporte a la automatización del proceso y a la evaluación del riesgo sistemático, pueda obtener y registrar detalles completos del cliente en un depósito común y brindar una visión única, amplia de las interacciones y actividad del cliente para las investigaciones y otros procesos comerciales de la DDC. Los sistemas automáticos de tecnología permiten una evaluación del riesgo activo, constante, de manera que la reevaluación del riesgo sea dirigida activamente por el sistema, a medida que sucedan las interacciones del cliente, se produzcan cambios en las conductas, y las políticas sean adaptadas para atender los cambios en los negocios y las necesidades regulatorias. Estos sistemas destacan los riesgos que necesitan una revisión manual y una mayor investigación por parte de los equipos de operaciones, para asegurar que los recursos sean bien administrados y los riesgos sean mitigados adecuadamente. Una plataforma común asegura y controla el acceso y también audita y registra los accesos e investigaciones, aplicando políticas comerciales y entregando la evidencia regulatoria de su implementación.

En una organización cuya estrategia está centrada en el cliente, los requisitos tecnológicos para una solución de la DDC son similares a las opiniones sobre el cliente requeridas por la gerencia de relaciones y la información almacenada puede dar apoyo a los procesos por fraude. Por ejemplo, si un cliente dijo que no usará canales de pago por Internet, ¿no debería utilizarse esta información para detectar anomalías o dar apoyo a las investigaciones de fraude más allá del alcance del ALD? Un sistema de tecnología y una plataforma integrada pueden dar beneficios adicionales a los negocios, permitiendo la reutilización de la información y brindando apoyo a las necesidades comerciales para realizar la evaluación del riesgo ALD, las evaluaciones del riesgo crediticio y la detección de fraude, CRM y otras actividades de comercialización. Por ejemplo, los clientes pueden volver a ser investigados con relación a los reportes ROS y los resultados de las investigaciones previas; las vinculaciones de los negocios y transacciones pueden ser entendidas mejor y los registros pueden ser conservados para los clientes internos y también para los terceros relacionados.

El futuro de la diligencia debida sobre el cliente

La diligencia debida efectiva sobre el cliente es la evaluación sistemática del riesgo de los clientes, les permite a las empresas que apliquen políticas basadas en el riesgo en todo el programa ALD. Las organizaciones cuya estrategia está centrada en el cliente están comenzando a reconocer cómo puede utilizarse la DDC para brindar información adicional del negocio y están utilizándolo como base para aumentar el conocimiento del cliente y mejorar las prácticas comerciales. Las empresas están buscando consolidar su opinión electrónica del cliente para permitir un enfoque holístico para hacer la evaluación de riesgo crediticio y ALD del cliente, tener información de la idoneidad del productos y otros elementos de la dirección del ciclo de vida del cliente.

El alcance de la diligencia debida sobre el cliente está ampliándose, casi todos los aspectos de la interacción comercial requieren algún nivel de diligencia debida. Las obligaciones anti-sobornos y anti-corrupción requieren una diligencia debida vinculada con las relaciones con los proveedores; las obligaciones de la Ley de Cumplimiento de Cuenta Fiscal Extranjera requieren que las instituciones financieras extranjeras refuercen sus procesos de diligencia debida para identificar a los titulares de cuentas estadounidenses; y la aplicación de métodos de detección de fraude giran sobre la obtención de información confiable, vinculaciones y análisis asociados con cuentas nuevas.

Lejos de ser una carga regulatoria, el futuro de la diligencia debida — para los clientes, proveedores y otras relaciones comerciales — está alojado en el corazón de las prácticas comerciales exitosas. Con el cumplimiento en primer lugar en términos de definición de los requisitos para los sistemas y procesos, las empresas deberían aprovechar esta oportunidad para crear mayores beneficios comerciales de los procesos y procedimientos ALD. Esto permitirá un enfoque integrado para mitigar los riesgos ALD y un enfoque holístico para conocer al cliente, impactando positivamente al final y obteniendo el apoyo ejecutivo de manera exitosa. A

Dr. Tony Wicks, director de AML Solutions, NICE Actimize, Londres, Reino Unido, Tony.Wicks@actimize.com

Los 10 mejores consejos sobre ciber-concientización para el profesional ALD

En los diez años desde el nacimiento de la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS), la tecnología digital ha crecido exponencialmente. Esta tecnología les ha dado a los profesionales ALD acceso a amplia gama de capacidades de investigación, análisis y reporte que son fundamentales para las operaciones y el cumplimiento con las leyes y regulaciones ALD. Sin embargo, el lado negativo de este poderoso recurso es el constante riesgo del ciberdelito tanto a nivel profesional como personal. Muchos lavadores usan Internet para crear o robar identidades personales o comerciales, comprometer información para ocultar sus actividades y atacar a aquellos que presentan el riesgo de provocarles el mayor perjuicio.

¿Es este un problema que permanecerá con nosotros mientras exista una? Sí. ¿Hay alguien que pueda sistemáticamente reconocer e impedir o mitigar estos riesgos? ¡Absolutamente! Probablemente usted vio a esa persona esta mañana mirándole desde el espejo del baño. La mayor defensa contra el ciberdelito es usted y sus mejores armas en este conflicto son la conciencia y la iniciativa personal.

Están aquellos que dicen que si usted agrega suficiente tecnología de seguridad en un problema de ciberseguridad, eliminará la amenaza. Estas son las mismas personas que prometen que puede eliminar el elemento o debilidad humana del proceso de seguridad. Para la persona promedio, la confianza de que la tecnología resolverá todo generalmente se disipa rápidamente cuando se corta un llamado en el teléfono celular, se rompe la computadora, el acceso a Internet es interrumpido o un asistente personal digital (PDA, por sus siglas en inglés) cae en un charco. Siempre está la pregunta de los recursos. Pocos pueden pagar el dinero y el esfuerzo de emplear la mejor, última y más amplia tecnología de ciberseguridad, especialmente en una economía incierta. Además, como muchos conocen por experiencia personal, al minuto después de haber comprador la última tecnología, se anunciará una alternativa más nueva, rápida y mejor. Con el crecimiento exponencial de la tecnología, la adquisición e implementación de tecnologías defensivas puede ser frustrante y un ejercicio que haga que no haya presupuesto que aguante.

El resumen es que cualquier clase de tecnología requiere la intervención humana, aún cuando no esté a nivel del usuario final. Las fallas en el desarrollo, implementación y mantenimiento crearán vulnerabilidades. Cuando un ciber-criminal va a trabajar, su único trabajo es encontrar y explotar estas vulnerabilidades.

La reacción a la realidad de las ciber-amenazas y los ciber-riesgos toma uno de tres caminos posibles. El primero es aplicar un enfoque anti-tecnología y no encender nunca un dispositivo digital. Esto no es práctico y ciertamente cada vez es más imposible en el mundo digital actual. El segundo es expresar desdén por todas las advertencias y arriesgarse a que estadísticamente, de los millones, tal vez miles de millones de dispositivos digitales, el suyo nunca será atacado. Hay un nombre para este grupo de gente: víctimas de ciber-delitos. El tercer enfoque es entender y aceptar los riesgos, asegurarse que las tecnologías, políticas y procedimientos defensivos sean empleados correcta y efectivamente, estar actualizado sobre las últimas amenazas y sobre cómo vencerlas o mitigarlas y finalmente, aceptar la responsabilidad personal por la ciber-seguridad de uno mismo.

Para aquellos en la arena ALD que están dentro de esa tercer categoría o que desean ser parte del pequeño conjunto de elite de los ciber-seguros, a continuación se incluye una lista de los 10 mejores consejos para reconocer o entender a las ciber-amenazas en un ámbito de cumplimiento. Antes de analizar la lista, entiendan que la elaboración de una lista de los diez más importantes de cualquier cosa, desde los mejores mariscales de campo de todos los tiempos de la NFL hasta las maneras más efectivas de realizar una entrevista de trabajo, siempre es subjetiva. Esto es especialmente cierto cuando se trate de ciber-seguridad y calidad de la información. Los marcos de referencia de este tema varían mucho. Un profesional de tecnología de seguridad de la información muy importante del sector privado tendrá una postura diferente de la de un especialista militar en ciber-seguridad. Si bien habrá muchos elementos en común en las dos listas, el enfoque de la evaluación, mitigación y defensa del riesgo/amenaza probablemente difiera, a veces drásticamente. Esa es la razón por la cual una pregunta en un motor de búsqueda de los 10 mejores consejos de ciber-seguridad lo llevará a conectarse con terabytes de información. La pregunta es, ¿qué es aplicable a usted y su trabajo?

Analizar los temas de ciber-seguridad a través de los ojos de un profesional ALD, sea que esté en cumplimiento, regulación o control legal, da, sin embargo, otro enfoque sobre el tema. El ámbito ALD conlleva su propio conjunto de riesgos y defensas. Esta lista trata de tomar eso en consideración. Algunos elementos de la lista son estratégicos, otros son estadísticos. Sin embargo, todos ellos le serán útiles en su trabajo y probablemente en sus actividades personales en Internet.

La Lista

10. Sepa que los malos siempre van a tener más recursos que usted. El mayor activo que usted tiene es usted. Una buena ciber-seguridad recae en la capacitación, vigilancia, dedicación y responsabilidad personal del individuo. Tomar en serio a la ciber-seguridad es la mejor defensa.
9. Sepa que los proveedores de ciber-seguridad solo pueden ayudar mucho. Ellos no pueden protegerlo de todo y si pudieran, ¿lo harían? ¿En interés de quién es tener una Internet comple-

Protegerse a sí mismo en línea es fundamental no solo para su vida personal, sino también para su efectividad como profesional ALD. Como se explicó en el artículo, hay muchas listas de los diez mejores con relación a la seguridad en línea. A continuación se indican los favoritos personales del autor. (Por favor tome nota del elemento de responsabilidad individual que está presente en todos).

1. Proteja con una clave todos los dispositivos y la red que almacena o permite el acceso a la información personal.
2. Encripte su información personal y sensible en los dispositivos móviles como los flash drives, los discos duros externos y los discos.
3. Cree claves difíciles (14-16 caracteres que incluyan letras mayúsculas y minúsculas, números y caracteres especiales como % o #) y cámbielos con frecuencia.
4. Apague las funciones de identificación geográfica que puedan identificar dónde se encuentra usted o dónde fue tomada la fotografía.
5. No deje sus claves y PINs expuestos a ojos entrometidos.
6. Utilice un software de ciber-seguridad probado (que incluya protecciones contra virus y otros malware y un protector fuerte) y manténgalo encendido y actualizado.
7. Organice reuniones familiares para analizar los temas personales. Mantenga informados también a sus amigos y compañeros de trabajo.
8. Realice auditorías regulares sobre ciber-seguridad de los dispositivos digitales de su familia.
9. Nunca divulgue los planes de viaje o sitios de contacto social haya que haya regresado usted de un viaje.
10. Aprenda cómo limpiar remotamente la información de los dispositivos perdidos que tengan esa capacidad.

Algunos podrán decir que muchos de los consejos en la lista son simplemente sentido común. Recuerdo, solo es sentido común cuando el sentido es común. Difunda la ciber-seguridad.

tamente segura? La tecnología es un aspecto integral de su ciber-defensa, pero nunca puede cubrir a todas las amenazas y riesgos. No deje que la tecnología lo deje satisfecho en sus interacciones en el ciber-espacio. Siempre se necesitarán la concientización personal y las prácticas cibernéticas seguras.

8. Conozca a las nuevas amenazas como los riesgos de las transferencias de dinero real en los mundos virtuales. No hay que pasar por alto las "pequeñeces". Esté atento a la gran cantidad de transacciones pequeñas, especialmente en el negocio de entretenimientos. Mientras usted está buscando la gran amenaza, la amenaza pequeña puede pasar desapercibida. Recuerde, esta amenaza no estaba ahí hace solo unos años. Manténgase informado sobre los últimos fraudes. Todo profesional ALD está tapado de trabajo, pero ignorar que los malos están actualizados podría tener consecuencias serias.

7. Sepa que los procedimientos de ciber-seguridad deben ser considerados tan seriamente como los procedimientos de cumplimiento. Romper las reglas de ciber-seguridad de una organización debería ser una infracción a la política de personal que merece sanciones severas. Permitir el acceso a la información o a las redes no es lo mismo que llevarse unas lapiceras extra del depósito de materiales o llegar tarde al trabajo. Las consecuencias de esos actos son demasiado importantes y potencialmente devastadoras. Sea un defensor de políticas y procedimientos de ciber-seguridad eficientes y razonables. Esté preparado para tomar las medidas correctivas o punitivas necesarias para aplicar esas políticas.

6. Sepa que las reglas de ciber-seguridad deben aplicarse a todos en la organización, sin importar el cargo que tengan. Prevenir que su red se vea comprometida al permitir el acceso a sus capacidades de información u operación es responsabilidad de todos. Tener un trabajo administrativo simple o estar sentado en una oficina importante no absuelve la responsabilidad de la ciber-seguridad. Se requiere solo un vínculo débil para hacer caer un sistema.

5. Sepa que la amenaza interna es mayor de lo que usted cree. La investigación muestra que la amenaza más importante a las redes y la información incluía a alguien con acceso interno. A nadie le gusta pensar que la persona que está en la oficina de al lado podría ser un ciber-lastre. El enojo, la enfermedad, la frustración y el desencanto pueden llevar a una persona a exponer un sistema o una red. De la misma que puede producirlo el chantaje o el robo de la ciber-identidad. Esto no significa que todos sus compañeros de trabajo vayan a ser mirados con sospecha, pero sí significa que las señales de advertencia no deberían ser ignoradas.

> Sepa que la amenaza interna es mayor de lo que usted cree

4. Sepa que la diligencia debida y la evaluación del riesgo no conocen fronteras en el ciber-espacio. Generalmente los criminales buscarán el camino de menor Resistencia. Sin embargo, cuanto mayor sea la recompensa, mayor será el trabajo que se tomen para obtener ese dinero. Si la creación de una identidad en línea multifacética elaborada les permite lavar millones de dólares, usarán el tiempo y los recursos. Parte de su evaluación del riesgo obviamente es decidir que tan lejos necesita investigar. Perfeccione esta habilidad. Reconozca que los criminales pueden querer crear una capa más de engaño digital que la inclinación o los recursos que usted tenga para investigar.

3. Sepa que al realizar las evaluaciones del riesgo, tiene que pensar como uno "malo" en un teclado sin límites de tiempo, dinero y equipo de computadora. Al crear sus ciber-defensas y evaluar sus actividades en línea pensando que "nadie nunca haría eso", podría quedar abierto a un ataque. Nunca subestime al enemigo.

2. Sepa que es muy importante como profesional ALD no estar comprometido personalmente en línea. Las fallas de ciber-seguridad personal pueden ser utilizadas en contra suyo y de su organización. Proteja su información de identificación personal, conozca los esquemas de *phishing* y aprenda a reconocer los sitios falsos de la web. No le de a los "malos" lo que necesitan para comprometer su trabajo como profesional ALD.

1. Finalmente, sepa. La sigla en inglés "SAR" a menudo es definida como la expresión en inglés *"Something Ain't Right"*, que quiere decir "Algo no está bien". Los esquemas de lavado de dinero son descubiertos por una "sensación instintiva" o un vacío en la lógica de la transacción. Lo mismo es cierto en línea. Si es demasiado bueno para ser verdad, es así. Si parece demasiado fácil, es así. Si la identidad de un riesgo identificado parece demasiado inocente, probablemente haya un problema. Confíe en los mismos sentidos que utiliza en su trabajo ALD cuando navega el ciber-espacio. Probablemente le impida caer en el engaño de una ciber-trampa.

Existen muchas otras palabras de la sabiduría de la ciber-seguridad que podrían tener un impacto más directo sobre su situación particular. Hay consejos disponibles que podrían referirse a cosas que usted ha visto afectan negativamente a su institución. Sin embargo, cualquiera sea su experiencia personal con el ciber-espacio, siempre será verdad que la mejor persona para mantenerlo seguro es la persona que está en el espejo, y el mejor consejo en esta lista de los 10 mejores consejos es el número 1: Siempre Sepa.

¿Cuál link es probable que sea parte de un fraude con phishing?

Número 1:
http://LincolnBankofNebraska.com
or
Número 2:
http://LincoInBankofNebraska.com

La respuesta se publicará en la edición de ACAMS Connection del 19 de octubre de 2011 de ACAMS Conexión.

Edwin (Ed) Beemer APR, CAMS, ALD/OFAC/BIS comunicaciones de cumplimiento y especialista en capacitación, jefe de equipo del programa de apoyo a la capacitación sobre Calidad de la Información y Ciber Seguridad, "Ciber-Patrullando" del U.S. Army's CIO/G-6 Cyber Directorate, Arlington, VA, EE.UU., efb@corpcommteam.com

Association of Certified Anti-Money Laundering Specialists®
ACAMS®

ACAMS GLOBAL TRAINING

OCTOBER – DECEMBER 2011

Build the Foundation for a Superior AML/CTF Program with ACAMS Training

go.ACAMS.org/AMLTraining

ACAMS WEB SEMINARS

Delivering cost-effective and top-notch training by veteran AML professionals

Special CASE STUDY Webinar

Wednesday, October 5, 2011 | 12:00 – 2:00 PM
The Team Approach to Winning the Compliance Race

Special FREE Webinar

Thursday, October 20, 2011 | 12:00 – 2:00 PM
Continuing the Good Fight: Next Steps to Combat Human Trafficking & Smuggling

Special CASE STUDY Webinar

Tuesday, October 25, 2011 | 12:00 – 2:00 PM
Choosing an Automated BSA/AML Monitoring System—A Banker's Perspective

Thursday, November 3, 2011 | 12:00 – 2:00 PM
Conducting Internet Investigations to Support Customer Due Diligence Processes

Wednesday, November 9, 2011 | 12:00 – 2:00 PM
Securities Focus for Introducing Broker-Dealers: CIP Challenges and Strengthening KYC, CDD and EDD Processes

Wednesday, November 30, 2011 | 12:00 – 2:00 PM
Fraud and Money Laundering: Detecting the Links in the Criminal Cycle

Friday, December 1, 2011 | 12:00 – 2:00 PM
Securities Focus: Understanding Recent Enforcement Actions on Micro-Cap and Low-Priced Securities

Wednesday, October 5, 2011 | 12:00 – 2:00 PM
Assessing Customer Risk for Corporate Clients: Understanding Shifts in Regulatory Expectations

ACAMS LIVE SEMINARS

Delivering a full-day of comprehensive, interactive training and networking

Conducting Effective AML Investigations: Law Enforcement Methodologies and Private Sector Techniques

San Francisco | October 19, 2011
Chicago | October 21, 2011

Speakers:

Dennis Lormel Retired FBI Agent Founder/President, DML Associates, LLC	Edward Rodriguez, CAMS Retired IRS CI Special Agent Principal, EORS Consulting, LLC

Asia-Pacific Region 3rd Annual Enhanced AML/CTF Tools & Techniques

Hong Kong | October 17, 2011

ACAMS LIVE CHAT

Delivering FREE regulatory & industry updates exclusively to ACAMS members

Special CASE STUDY Live Chat

Wednesday, October 26, 2011 | 12:00 – 2:00 PM
Emerging Trends in Financial Crime: Counterfeit Trade—The Next Big Threat

Wednesday, December 14, 2011 | 12:00 – 2:00 PM
Understanding the Challenges and Opportunities of Global Banking and Trade-Based Finance

ON-DEMAND TRAINING:

Choose from a library of over 90 previously recorded web seminars from the convenience of your desk, at a time of your choosing. On-Demand training offers flexible, comprehensive options to meet your training goals.

Visit go.acams.org/AMLtraining for full descriptions and registration.
You may also contact an ACAMS representative directly at +1 305.373.0020 or info@acams.org.

Combatiendo al crimen organizado a la antigua: Un estudio sobre Al Capone

La mayoría de las principales ciudades del mundo han designado a grupo de funcionarios de control legal para identificar, tener como objetivo y desmantelar a los Sindicatos del Crimen Organizado (OCS, por sus siglas en inglés). Generalmente, la ofensiva general de los esfuerzos policiales es desmantelar a un OCS mediante el arresto y condena de sus líderes. Con frecuencia, puede llevar años desarmar totalmente las poderosas estructuras de los OCSs, y al mismo tiempo, lamentablemente algunos OCS pueden seguir creciendo a pesar de los mejores esfuerzos de las autoridades de control legal. El desafío de llegar hasta la cima a menudo está basado en la eliminación de la distancia entre los perpetradores del crimen y los directores que se beneficiaron de él. ¿Cómo es posible llegar hasta la punta de un OCS sabiendo que los asociados criminales prefieren ir a la cárcel antes que "delatar" a sus hermanos, especialmente a sus jefes?. Ésta es una pregunta muy antigua que afortunadamente tiene una respuesta antigua: Al Capone.

Al final, la condena de Al Capone (también conocido como "Cara Cortada") fue mucho más compleja que un caso penal aislado sobre impuestos. El Servicio de Rentas Internas (Internal Revenue Service, o, IRS, por sus siglas en ingles) publicó recientemente el informe de la investigación en el que se revelan cientos de detalles referidos al caso completo contra Capone. Ese informe, junto unas memorias descubiertas recientemente escritas por el agente del IRS a cargo de la investigación sobre Capone, demuestran lo difícil que fue realmente capturar al Enemigo Público Número 1. De particular importancia actual son las técnicas de investigación financiera utilizadas para condenar a Capone en los años '30, que engloban a los métodos que pueden utilizar actualmente las autoridades de control legal.

Ilustración por Victoria Racine

Las técnicas utilizadas naturalmente incluían a algunos de los métodos que uno podría esperar. Los investigadores financieros analizaron enormes cantidades de registros comerciales y trataron de rastrear los gastos extravagantes realizados por Capone, pero no estuvieron ni cerca de ser suficiente. Para atrapar finalmente a Capone tuvieron que descubrir cuentas bancarias nominadas, rastrear transferencias de dinero ocultas hechas en Western Union, descubrir a intermediarios, encontrar y convencer a testigos reticentes, así como también utilizar a informantes y agentes encubiertos. Todo el tiempo, estos valientes investigadores recibieron amenazas de muerte, intentos de manipulación del jurado a través de amenazas o sobornos e intimidación abierta de testigos.

El IRS no podía usar solo esto y no lo hizo. El análisis de los pasos de cómo fue atrapado Capone ilustra cómo los bancos y negocios de servicios monetarios fueron abusados para ocultar el dinero de Capone, en una manera bastante similar a la del escenario actual. Como verán, las ganancias obtenidas ilegalmente por Capone fueron transferidas a través de un banco pequeño y de Western Union, no solo en su nombre. Pero primero, para entender porqué el gobierno federal persiguió a un mafioso de Chicago, ayudará explicar quién era él realmente en ese momento.

¿Quién fue Al Capone?

A lo largo de los años, Hollywood ha cubierto de glamour a los gángsters de los años '20 y a veces incluso ha descripto a Al Capone como un héroe de clase. En realidad, Capone supervisaba una enorme y despiadada organización criminal que operaba con impunidad en Chicago. Las películas mostraron algunos de los crímenes de Capone de manera precisa, desde el contrabando de cerveza y whisky hasta el manejo de casinos ilegales y casas de prostitución. Sin embargo, la banda de Capone también se diversificó en otras actividades más viles, que incluían la extorsión, secuestros y chantaje. Hollywood pareció pasar por alto el hecho de que Capone y su grupo mafioso pelearon a su estilo hasta llegar a ser la banda criminal más importante de Chicago asesinando a entre 40 y 50 de sus rivales. Claramente esta clase de delito fue un gran problema, no solo para las bandas rivales, sino también para los ciudadanos comunes de Chicago. Los ciudadanos estaban indignados con la Masacre del Día de San Valentín en 1929, culpando por el golpe directamente a la banda de Capone.

La caída de Capone comenzó con la autodesignada Comisión del Crimen de Chicago (CCC), un grupo de seis acaudalados empresarios. Temiendo que no tuvieran ninguna opción viable a nivel local, la CCC le pidió directamente al presidente Herbert Hoover que trasladara recursos del gobierno federal. El presidente Hoover posteriormente inició una replica muy pública proclamando a Capone el "Enemigo Público Número 1". Hoover instruyó luego a varias agencias federales, incluida la Oficina de Prohibición, para que se concentraran en Capone y su OCS. Finalmente, sin embargo, fue la Unidad de Inteligencia del IRS (la precursora de Investigaciones Criminales del IRS Criminal) la que fue fundamental en el futuro encarcelamiento de Capone. De acuerdo con el edicto de Hoover, la Oficina Central del IRS rápidamente reclutó al Agente Especial Frank Wilson para que se trasladara a Chicago y dirigiera un equipo de Agentes Especiales del IRS para "Atrapar a Capone".[1] Los desafíos que enfrentó Wilson entonces eran importantes y sorprendentemente similares a los desafíos que existen hoy para investigar a los líderes de los OCS actuales.

¿Dónde empezar?

Wilson rápidamente determinó que Capone vivía una vida de lujo, aunque de acuerdo con los registros conocidos, Capone solo era dueño de una modesta casa en los suburbios de Chicago. No tenía ningunos otros bienes a su nombre, no tenía cuentas bancarias ni acciones y Capone nunca había presentado declaraciones de impuestos. Wilson señalaba en sus memorias, "…no había ninguna pista de que ningún dólar de sus palacios de juegos, sus salas de apuestas a carreras de caballos, los burdeles o las actividades de contrabando directamente o indirectamente llegaran alguna vez a sus bolsillos".[1] Capone tuvo la audacia de pasar los inviernos en Miami, viviendo en una mansión en el canal intercostal.

En un acuerdo nada ortodoxo, algunos periodistas de diarios tuvieron acceso directo a Capone, detallando fragmentos de su vida de gángster y mostrándolo como un rebelde audaz. Fue sorprendentemente fácil saber que Capone organizaba fiestas fastuosas, gastaba dinero extravagantemente, y entregaba obsequios (y sobornos) sin ninguna dificultad. Sin embargo, el tema más problemático para Wilson era que no había testigos de los gastos e ingresos de Capone.

Wilson sabía muy bien que posibles testigos conocían bien las actividades financieras de Capone, pero también estaban legítimamente muertos de miedo para hablar de ello. Uno de los posibles testigos le dijo a Wilson, *"Si le cuento a usted sobre Capone y su redada, Cara Cortada me liquida o va a dañar a mi familia …"*. Esto puede sonar lamentablemente repetido para los oficiales de los grupos de trabajo actuales. Entonces, ¿cómo actuaría usted en este punto? Veamos cómo lo hizo Wilson.

Encontrando evidencia

Wilson tenía que superar dos obstáculos para atrapar a Capone. Primero, tenía que encontrar una manera de obtener evidencia financiera cuando la mayoría de las transacciones de Capone eran en efectivo. Segundo, una vez que Wilson localizara esa evidencia, necesitaba encontrar una manera de persuadir a los testigos para que declararan contra Capone.

Igual que hoy, los casos criminales relacionados con impuestos requerían la prueba de que fondos rastreables en determinados años eran, de hecho, ingresos derivados de impuestos vencidos y adeudados. Wilson explicaba en sus memorias, "Llegar hasta el fondo de las actividades financieras de la mafia de Capone y determinar el ingreso gravado de Cara Cortada fue como resolver varios rompecabezas terriblemente difíciles, cada pieza representaba una rama diferente del negocio de la mafia".[1]

Si bien la cronología exacta del caso no es conocida, se sabe que Wilson comenzó su trabajo en algún momento de 1929. Wilson y su equipo trabajaron durante cerca de un año tratando de encontrar transacciones que pudieran vincularse a los ingresos de Capone. Wilson se lamentaba, "[Nosotros] íbamos a los bancos, las agencias de crédito y los ingresos de otras posibles fuentes, tratando de encontrar algún registro de las transacciones comerciales que vincularan a Cara Cortada. Ni siquiera uno".[1]

Dado que no tenía suerte con Capone individualmente, Wilson inició el siguiente paso lógico, una investigación dentro del OCS de Capone. El equipo de Wilson dirigió su atención a las posibles violaciones impositivas de los lugartenientes de Capone. Como regla

[1] Jonathan Eig, "Get Capone: The Secret Plot That Captured America's Most Wanted Gangster" *("Atrapen a Capone: El Complot Secreto que Capturó al Gángster Más Buscado de EE.UU.")* (2010),

general, los camaradas criminales a menudo tienen un mejor recuerdo de los hechos cuando se enfrentan a largas condenas en prisión, especialmente si sus jefes continúan libres. El equipo del IRS cosechó un éxito inicial con esta estrategia y rápidamente obtuvo declaraciones de culpabilidad o condenas por violaciones al impuesto a las ganancias en el círculo íntimo de Capone. El segundo al mando de Capone, Jack Guzik (responsable de los juegos de apuestas y la prostitución), fue condenado a cinco años; Ralph Capone (el hijo mayor de Al y responsable de la distribución y fábricas de cerveza) recibió una condena de tres años; y Frank Nitto (el que hacía cumplir los acuerdos por la fuerza y era responsable de la distribución de alcohol) fue condenado a 18 meses. Desafortunadamente, ninguno de estos hombres se volvió en contra de Capone.

El primer gran quiebre

En el segundo año de la investigación, Wilson y su equipo analizaron la evidencia que no habían revisado de sus anteriores allanamientos, memorandos voluminosos y otros informes, sin mucho éxito. Un día tarde, por casualidad Wilson encontró el quiebre que necesitaba. Accidentalmente descubrió algunos sobre marrones con polvo atados con una cinta en lo que pensó sería un archivo de carpetas sin usar. Wilson señaló, "Algo me llevó a examinarlo y entonces corté la cinta y me encontré sosteniendo tres libros de contabilidad, negros con puntas rojas".[1] Después de analizar rápidamente los libros Wilson calculó que mostraban cerca de US$540.000 en ganancias netas probablemente de uno de los casinos de Capone. Fue un descubrimiento importante pero solo era la mitad de su objetivo. Su desafío real sería la otra mitad, encontrar a testigos que declararan sobre ellos.

Wilson supo que los libros de contabilidad habían sido decomisados en una redada en el establecimiento Hawthorne Smoke Shop (HSS) en 1926. Una serie de entrevistas posteriores revelaron que el HSS era el negocio pantalla del palacio de apuestas más grande de Cicero, un arenoso suburbio de Chicago. Wilson hizo que varios testigos presentaran los libros de contabilidad como evidencia y que dieran otra declaración testimonial vital. Uno de los testigos clave recordó que al comienzo del allanamiento Capone decía alegremente, "Debería ser mi fiesta. Yo soy dueño del lugar".[1] Si bien eso ayudó, ninguno de ellos pudo declarar sobre el componente más importante de todos, la importancia de los registros en los libros.

Wilson creía que la mayoría de los asientos contables registrados en el libro estaban hechos por la letra manuscrita de la misma persona, ¿pero de quién era? Wilson dirigió un proceso trabajoso para reunir muestras de letra manuscrita de todo matón en Chicago. Wilson indicó que tomó muestras de los "registros de votos en los distritos electorales, de las cuentas de ahorro, de los tribunales policiales y de los recibos de las cadenas que firmaban cuando eran esposados".[1] A través del proceso de eliminación, encontraron una coincidencia con el libro en una sola boleta de depósito de un banco en Cicero. El testigo era Lew Shumway, aunque como podía predecirse, no se lo pudo encontrar en ningún lado.

Wilson sospechaba que Capone, que estaba en Miami porque era invierno, mantenía cerca a Shumway. Wilson se trasladó rápidamente a Florida y descubrió a Shumway trabajando en las cajas de una pista de carreras de perros. Wilson se acercó a Shumway y le presentó una difícil opción. Elegir a Capone o elegir al gobierno con la promesa de Wilson de darle protección. Shumway eligió al gobierno y dio una declaración testimonial para el caso. Shumway explicó que Capone era uno de los verdaderos dueños del HSS. Shumway pudo rendir cuentas sobre 18 meses de ganancias diarias en el casino y las consecuentes ganancias que podían ser acreditadas a Capone individualmente. Wilson supo que finalmente tenía al testigo para atrapar a Capone y recordó, "Esa noche saqué tan rápidamente a Shumway fuera de Miami que incluso su esposa creyó que iba a visitar a un familiar enfermo en Oklahoma".[1]

Más testigos

Si bien Shumway era ciertamente un testigo de mucho valor para el caso, al mismo tiempo también se buscaron otras fuentes de evidencia financiera. Dos intrépidos agentes del IRS contactaron a bancos locales para ver si podían encontrar alguna vinculación con la banda de Capone. Los agentes descubrieron que desde 1926 hasta 1928, casi la mitad de los cheques de cajero emitidos por el Banco Pinkert State habían sido adquiridos por un tal "J. C Dunbar". Un análisis más detallado mostró que estos cheques eran endosados por el hombre que se ocupaba de las finanzas de Capone, Jack Guzik, o por Dunbar mismo.

Un ex cajero del banco Pinkert reveló que J. C Dunbar era en realidad un alias de Fred Reis. El cajero dijo que Reis era cajero en el casino de Capone conocido como The Ship. The Ship era el sucesor de HSS, al que se le había dado un nuevo nombre después del raid mencionado realizado en 1926. El cajero le dijo a Wilson, "Seguro, todos en el banco conocían a Dunbar [también conocido como Reis]. Él venía casi todos los días. Siempre queríamos atenderlo porque nos daba una propina de US$5 cada vez que compraba un cheque de cajero o hacía otra operación en el banco".[1] El cajero además explicó que Reis tenía muchas cuentas en el Pinkert con tres alias distintos. El cajero señaló, "Los cambiadores de cheques y los oficiales lo llaman Señor Dunbar. Nosotros los cajeros lo llamamos Fred".[1] No fue una sorpresa que Reis tampoco fuera encontrado en ningún lado.

Wilson supo por sus informantes que Reis estaba viviendo desapercibidamente en St. Louis. Wilson y otro agente viajaron de noche a Missouri para encontrar a Reis. Una hora antes de que llegaran los agentes, Reis había recibido un paquete de la organización mafiosa con dinero en efectivo e instrucciones para abandonar el medio-oeste inmediatamente. Wilson intervino y durante los siguientes cuatro días convenció a Reis para que cooperara. Wilson llevó a Reis de vuelta a Chicago y contó en sus memorias, "Allí, dio una declaración fundamental que había estado esperando, la cual puso las enormes ganancias de The Ship directamente en los bolsillos de Capone".[1] Reis fue también incluido en una especie de protección de testigos de los años '30 y fue enviado a Sudamérica hasta que se lo necesitara para el juicio a Capone.

Transacciones ocultas

En esencia, Capone tenía el mismo problema que los criminales de hoy en día; Capone tenía que confiar en otras personas para mover o gastar su dinero. Y esa confianza se convirtió en una de las mayores vulnerabilidades de Capone. Junto con sus banqueros y tenedores de libros en los que confiaba, Capone necesitaba asociados leales para movilizar su dinero. Por ejemplo, la mansión en Miami no estaba a nombre de Capone. La mansión había sido adquirida por un

[1] Jonathan Eig, "Get Capone: The Secret Plot That Captured America's Most Wanted Gangster" *("Atrapen a Capone: El Complot Secreto que Capturó al Gángster Más Buscado de EE.UU.")* (2010),

testaferro utilizando el dinero en efectivo de Capone. El comprador registrado de la mansión de Capone era Parker Henderson, el hijo de un ex alcalde de Miami.

Además, los empleados de la casa de Capone retiraban transferencias de dinero hechas en Western Union a su nombre y utilizaban los fondos para tareas de paisajismo, mantenimiento y remodelaciones. Esto fue importante durante el juicio a Capone, ya que un representante de la oficina de Western Union en Miami le dijo al jurado que ella había sido, "instruida por Capone para pagarlas [las transferencias de dinero] cuando las mismas fueran presentada por algún miembro de su casa".[2] Estas transferencias sumaban hasta US$72.230 de los ingresos de Capone.

Pistas como estas fueron posibles porque Wilson tenía un agente encubierto del IRS dentro del OCS de Capone. Mientras que Capone y su extensa banda vivían en el Hotel Lexington, el Agente Especial Mike Malone eligió simplemente merodear en el lobby del hotel y esperar pacientemente a que los hombres de Capone lo llevaran hasta él. Malone eventualmente se ganó toda la confianza y fue invitado a cenar con Capone y su banda. Malone informó comentarios estratégicos de Capone y los miembros de la banca a Wilson. Las observaciones de Malone desde el lobby del hotel ayudaron a Wilson a encontrar a testigos que eran difíciles de encontrar. Además, los informes de Malone relacionados con el momento exacto de los telegramas de Western Union desde el hotel, a menudo se correspondían con transferencias de dinero posteriores.

El Capone real

Capone conocía la investigación del IRS y contrató a un abogado defensor de alto perfil para contactar a la agencia y pedir una resolución del caso. El equipo de la defensa de Capone ofreció US$500.000 al IRS para cerrar el caso. El IRS rechazó la oferta, pero terminó en una sesión cara a cara en las oficinas del IRS con Capone y su abogado. Al final de la improductiva entrevista y sin ningún testigo alrededor, Capone presentó un puñado de cigarros y le preguntó a Wilson, "¿Fuma?" Wilson respondió, "No". Capone respondió, "Alguien está tratando de zarandearme. Me voy a cuidar. Cuídese, Wilson". Wilson respondió rápidamente, "Seguro que lo haré".[1]

La amenaza velada de Capone era fuerte y posiblemente pudo haber sido letal si no hubiera sido por el uso de informantes por parte de Wilson. Wilson recordaba, "Yo siempre había sido amigable con los reporteros en el pasado. Algunos de ellos me habían pasado muy buenos datos que probaron ser extremadamente valiosos". La necesidad de informantes llevó a Wilson hasta Eddie O'Hare. Wilson más tarde escribió, "… las pistas y el consejo … de Eddie fueron de tan enorme importancia que las considero el factor más importante que culminó en la condena de Al Capone".[1] Wilson indicó que O'Hare le dijo chismes como, "Prueba con este banco o abandona eso; está lleno de dinamita y podrías estar alertando a".[1] No obstante, O'Hare advirtió seriamente a Wilson que Capone había ordenado matar a Wilson y el equipo de fiscales dos semanas después de la advertencia de Capone. O'Hare también describió un increíble esquema de manipulación de los jurados urdido antes de que comenzara el juicio.

Además de la evidencia y la declaración de los tenedores de libros, el equipo necesitaba demostrar cómo Capone había gastado una suma correspondiente de dinero durante esos mismos años. Era un desafío enorme porque, "…con la excepción de las transferencias cablegráficas de dinero de Western Union y un cheque ocasional, [Capone] realizaba todas sus transacciones financieras en efectivo".[1] A pesar de los obstáculos, los investigadores descubrieron recibos y encontraron a los testigos necesarios para documentar fiestas lujosas, ropa cara y facturas de hotel exorbitantes. Estos gastos incluían la compra de numerosos vehículos, dos Yates, la mansión en Miami y mucho más. Finalmente el equipo de la fiscalía estaba listo.

El juicio

En junio de 1931, Capone fue acusado de 22 cargos por violaciones impositivas que iban desde el año 1924 inclusive hasta 1929. La acusación indicaba que Capone había ganado US$1.055.375 durante esos años (utilizando el Índice de Precios al Consumidor esa suma equivaldría a US$13.400.000 de la actualidad).

Durante el juicio en octubre de 1931, Shumway detalló las ganancias y pérdidas diarias encontradas en los asientos del libro diario escritos por él, así también como el porcentaje que tenía Capone de sus ganancias en el HSS desde 1924 hasta 1926. Mientras Reis daba cuenta de los ingresos de Capone mediante la compra y distribución de cheques de cajero a nombre de nominados en 1927. Otros testigos confirmaron el control que tenía Capone sobre el HSS y el The Ship durante esos mismos años. Muchos otros testigos fundamentales, que incluían a banqueros, empresarios y empleados de negocios de servicios monetarios, declararon acerca de los gastos extravagantes de Capone y el uso que hacía de nominados.

El jurado declaró a Capone culpable de tres cargos de evasión fiscal en los años 1925, 1926 y 1927 y de dos cargos menores por no presentar declaraciones de impuestos en 1928 y 1929. Capone fue sentenciado a 11 años de prisión por las violaciones y fue uno de los tristemente célebres primeros prisioneros en ser enviados a Alcatraz, donde cumplió la mayor parte de su condena.

Los desafíos de hoy

Para los investigadores actuales, el desafío de demostrar la propiedad de los ingresos o fondos criminales es el mismo que existía en la década de 1920. A veces, parece imposible rastrear las fuentes de ingresos en efectivo o gastos que parecen imposibles de rastrear, hacer que declaren testigos reticentes u hostiles o descubrir a los testaferros. Estas dificultades pueden superarse, pero las autoridades de control legal no lo pueden hacer solas. Como se demostró en nuestro repaso histórico de las técnicas empleadas por Wilson y su equipo de investigadores, se necesita la cooperación del sector privado. Los negocios, las instituciones financieras y los negocios de servicios monetarios son testigos comprometidos, así como también los informantes de la actualidad. Los Reportes de Operaciones Sospechosas (más de 1,3 millón son presentados cada año en los EE.UU.) ayudan a los oficiales de control legal en formas que Eddie O'Hare y Mike Malone jamás podrían haber imaginado. Como Wilson proclamó en sus memorias hace 60 años, "Las agencias de control legal no pueden funcionar sin cooperación y este hecho no puede ser expresarse con demasiada frecuencia o demasiado forzadamente". A

Mark Weber, agente especial, IRS, San Francisco, CA, EE.UU., mark.weber@ci.irs.gov

[1] Jonathan Eig, "Get Capone: The Secret Plot That Captured America's Most Wanted Gangster" *("Atrapen a Capone: El Complot Secreto que Capturó al Gángster Más Buscado de EE.UU.")* (2010),

[2] IRS — Intelligence Unit, Summary Report: Alphonse Capone Investigation, et al. (December 21, 1933). http://www.irs.gov/pub/irs-utl/file-2-report-dated-12211933-in-re-alphonse-capone-by-sa-frank-wilson.pdf

Convergencia de Crímenes Financieros

El caso de la integración de los procesos de fraude y antilavado de dinero

La tormenta perfecta de las mayores presiones regulatorias y los ataques sofisticados, de alta velocidad, de fraude, han creado una oportunidad para los departamentos de fraude y cumplimiento para unir los presupuestos y los recursos, así también como para adoptar nuevas tecnologías para reducir la exposición al riesgo financiero y reputacional. El objetivo de este artículo es destacar la justificación cualitativa y financiera para fusionar los procesos de fraude y antilavado de dinero hacia un modelo operativo de crímenes financieros.

Abriendo las líneas de comunicación

Durante varios años, la industria de servicios financieros ha debatido las ventajas de unir los procesos antifraude y ALD bajo un paraguas común de crímenes financieros. Pero, cada vez más y más, las instituciones financieras se están dando cuenta que una visión holística de la conducta sospechosa del cliente — en todas las líneas de productos y servicios — puede traducirse en investigaciones más efectivas y eficientes, mejorando la colaboración entre los departamentos, eliminando las investigaciones redundantes e identificando los riesgos que no serían detectados por tener procesos y herramientas separados.

En diciembre de 2010, la Asociación de Especialistas Certificados en Antilavado de Dinero y Ernst & Young publicaron una encuesta conjunta realizada a encuestados globales de instituciones financieras, agencias de control legal y regulatorias. La encuesta — titulada "Vinculando a los Programas Antifraude y Antilavado de Dinero: ¿Oportunidad No Realizada o Complejidad Innecesaria?" — reveló que el 52% de las firmas de servicios financieros ya habían integrado algunos aspectos de sus funciones ALD y antifraude. Más aún, el 64% de las agencias gubernamentales recomendaba que las instituciones financieras aplicaran un enfoque más concertado respecto de los crímenes financieros.

La creciente obligación de convergencia

Varias publicaciones han apoyado el caso de la convergencia de los procesos de los crímenes financieros, incluidas: el lavado de dinero y la correlación con el fraude destacada en *Mortgage Loan Fraud Connections with Other Financial Crime (Conexiones del Fraude con Préstamos Hipotecarios con Otros Crímenes Financieros)* de la Red de Control de Crímenes Financieros de los EE.UU. (FinCEN, por sus siglas en inglés); el informe del Grupo Wolfsberg sobre sinergias entre los riesgos de fraude con tarjetas de crédito y el lavado de dinero, la Guia ALD del Grupo Wolfsberg *(Wolfsberg AML Guidance)*; y la Guía de Asesoramiento de FinCEN titulada *Guía para Instituciones Financieras sobre Acontecimientos Recientes en Siria (Guidance to Financial Institutions on Recent Events in Syria)* que asesora sobre la diligencia debida reforzada de las personas expuestas políticamente sobre el movimiento de bienes fraudulentos o apropiados indebidamente.

De acuerdo con un informe de administración de casos del Tower Group, una importante firma consultora y de investigaciones especializada en la industria de servicios financieros globales, "las demandas de una mayor visibilidad y transparencias en riesgos de todas las formas, nuevos mandatos de los directores respecto de la reducción del riesgo, y las obligaciones regulatorias que

provienen de otras partes del negocio, todas ellas ponen de relieve la necesidad de un enfoque más holístico para administrar el riesgo y el fraude"[1].

Todo esto — así como también una expectativa por parte de los gobiernos y los reguladores de que los investigadores de fraude sepan cuando un sospechoso esté siendo investigado también por otro área dentro de la institución — obligará a las instituciones financieras a dejar de trabajar en silos separados y compartir los recursos y procesos para optimizar mejor la detección de los crímenes financieros.

Los defraudadores creativos a menudo diseminan sus actividades criminales en los productos y transacciones, haciendo que cada actividad parezca inocua. Colectivamente, esas actividades representan pérdidas importantes que pueden ser evitadas con el conocimiento previo de los casos investigados en otros sectores. Con los departamentos de crédito, tesoro y ALD, por ejemplo, trabajando en forma separada — con sus propias soluciones puntuales para administrar y reportar sobre los casos — existe una escasa comunicación entre los equipos y a menudo hay una reticencia a compartir lo que se consideran informaciones propias.

Recientemente repasamos un proyecto con un banco asiático que analizaba la información de distintos canales para detectar operaciones del crimen organizado. En una operación en particular, el banco ya había identificado a tres de los sujetos con sus sistemas de alerta de fraude existentes. Cuando aplicamos análisis de redes para incluir información de las transacciones y datos demográficos, pudimos identificar a seis individuos más que compartían domicilio en común, empleadores en común y fecha de nacimiento en común. Cuando revisamos sus transacciones, las mismas estaban siendo realizadas en efectivo, cheques, transferencias y operaciones en cajeros automáticos a través de canales de cajeros automáticos y teléfono. Ellos mostraban una variedad de comportamientos de fraude y estructuración. En ausencia de otra información, su conducta parecía benigna. Sin embargo, cuando revisamos la operación holísticamente, había una exposición al riesgo de medio millón de dólares por posibles créditos incobrables. En este ejemplo, aumentamos nuestra detección de fraude aplicando un enfoque holístico. Como resultado de ello, el jefe del grupo de seguridad de la institución tuvo la justificación para crear una nueva función de investigación dedicada a las operaciones organizadas, independientemente de una tendencia de fraude o ALD.

Si bien la idea de combinar los procesos antilavado de dinero y antifraude puede a primera vista parecer una tarea dantesca, especialmente para las instituciones pequeñas y medianas, no significa necesariamente reorganizar o fusionar los departamentos creados para lograr mejoras en eficiencias y efectividad. Mucha de la información requerida para detectar lavado de dinero es similar a la información que se requiere para impedir las transacciones fraudulentas. Si bien los procesos y el flujo de trabajo para administrar las alertas de fraude y ALD son muy diferentes, la mayoría de las instituciones están consolidando las investigaciones en una plataforma unificada para eliminar los análisis redundantes de los sujetos. Los profesionales ALD deberían funcionar bien en este modelo operativo dado que los investigadores de lavado de dinero a menudo abarcan múltiples partes, cuentas y productos

Administración de casos de empresas

La convergencia puede definirse como el movimiento coordinado de dos ojos o la fusión de distintas tecnologías. Un enfoque pragmático es empezar primero con un modelo de "dos ojos" que utilice la tecnología de administración de casos de empresas *(enterprise case management*, o ECM, por sus siglas en inglés) para ayudar a los investigadores a conectar los puntos entre las conductas sospechosas y los clientes. Una vez que analizamos la conducta ilícita de un sujeto en toda la empresa, tenemos una visión más exacta de las exposiciones al fraude y a menudo detectamos relaciones del clientes que habían estado ocultas previamente y que podrían representar un riesgo reputacional importante.

> Los defraudadores creativos a menudo diseminan sus actividades criminales en los productos y transacciones

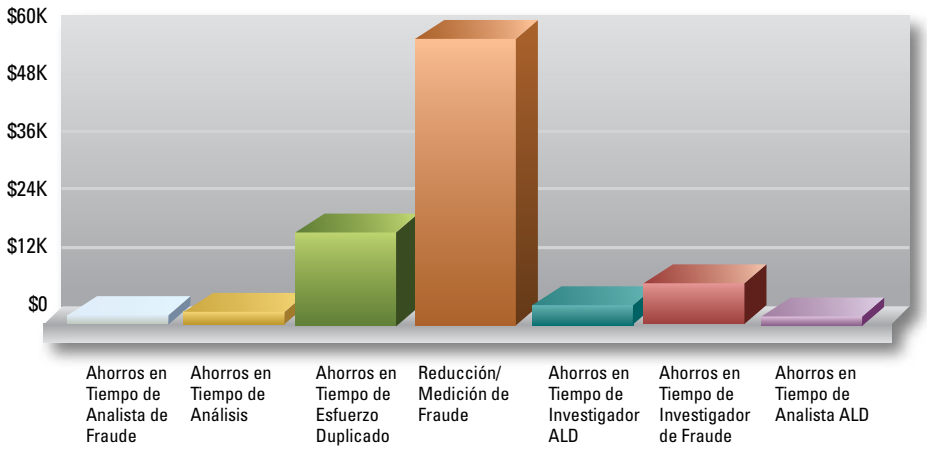
Al consolidar los alertas de muchas fuentes, los sistemas ECM permiten investigaciones eficientes a través del análisis en todos los departamentos de la información de las transacciones y otros datos de las cuentas. Con más información a disposición, los investigadores resuelven los alertas más rápidamente. En los casos que incluyen tipologías más sofisticadas, los sistemas ECM le permiten al investigador ver todos los alertas de fraude y ALD sobre el sujeto, mejorando así la precisión de las decisiones. La mayoría de las instituciones financieras ya han invertido en aplicaciones de software para el análisis de lavado de dinero y fraude, y, dado el clima de crisis económica actual, no cae bien "quitar y reemplazar" los sistemas vigentes. Sin embargo, la última generación de sistemas ECM puede aceptar alertas de distintos sistemas, aplicar la lógica de administración de alertas para calificar y atender el alerta y brindar una visión de la empresa de los riesgos existentes en el portafolio, geográficos y la dimensión del cliente. En esencia, las nuevas tecnologías pueden incrementar los sistemas existents para entregar una mejora marcada.

La mayor cantidad de procedimientos de control ha incrementado la importancia del gobierno y auditoria de las investigaciones para asegurar la adherencia consistente a las políticas y procedimientos. Los flujos de trabajo estructurado brindan controles para regir los requisitos de los procesos de investigación. La habilidad para explicar las decisiones y entregar informes gerenciales sobre tendencias y resúmenes es crucial para administrar el riesgo en todas las exposiciones a los crímenes financieros. Los sistemas ECM ofrecen reportes gerenciales y tendencias de las principales estadísticas operativas, incluyendo volúmenes, recuperos, antigüedad de los casos, presentaciones de ROSs y exposiciones. A la luz de los riesgos dinámicos de fraude y las expectativas regulatorias, las instituciones financieras necesitarán un sistema que sea ampliable, interoperable y altamente flexible.

Justificación financiera — Un modelo de caso de negocios

Una institución financiera puede justificar fácilmente la adopción de un enfoque de crímenes financieros cuantificando los

[1]The Tower Group. La Evolución de la Administración de Casos: *La Convergencia del Fraude, el Riesgo y la Administración de Oportunidad (The Evolution of Case Management: Converging Fraud, Risk, and Opportunity Management)*, Rodney Nelsestuen. Agosto 2009.



ahorros en los costos y las mejores tasas de detección. En este ejemplo, un banco holding mediano quería determinar los ahorros y el retorno de la implementación de un sistema ECM como primer paso para su instalación de una plataforma de crímenes financieros en la empresa. Durante el ejercicio, citamos varios beneficios financieros, incluida la consolidación del sistema, la reducción de los costos en personal IT, así como también la reducción de los aranceles por mantenimiento de software mediante la eliminación de sistemas redundantes. Sin embargo, el cliente quería focalizarse en los beneficios directos para el proceso de investigación financiera. En nuestro estudio acordamos medir los siguientes beneficios:

Eficiencias de investigación mejoradas

- Mayor velocidad de la investigación porque el sistema muestra todos los alertas para un sujeto al analista, elimina la necesidad de investigaciones a los sistemas de registro y automatiza el llenado de los campos fundamentales.

Mayores tasas de detección de fraude

- A menudo, los eventos de escaso valor no son registrados y medidos como fraude. El sistema acumula las exposiciones que no hubieran sido captadas y medidas previamente.

Eliminación del esfuerzo duplicado

- Ahorros en los costos debido a la eliminación de las revisiones duplicadas de alertas y las investigaciones de casos de sujetos en común y la eliminación del reingreso de información.

Mejores funciones de reporte y de auditoría

- Reducción en la cantidad de horas necesarias para generar reportes sobre exposiciones al riesgo, presentaciones, pérdidas y mediciones operativas.

Para preparar el caso de negocios, medimos el costo anual extendido de cada uno de sus analistas e investigadores; el promedio anual de horas dedicadas a las investigaciones, la cantidad de investigaciones, la eliminación esperada de trabajo duplicado, y el aumento esperado del fraude detectado. El siguiente cuadro incluye las expectativas conservadoras entregadas por el cliente:

Rol	Equivalente Tiempo Completo o Empleados	Porcentaje de Mejora
Analista ALD	3	15%
Analista Fraude	3	15%
Investigador ALD	5	15%
Investigador Fraude	8	15%
Análisis/Reporte	3	20%
Eliminación de Esfuerzo Duplicado	22	15%
Tasas de Detección de Fraude	ND	10%

Para esta Unidad de Investigaciones Financieras integrada por 19 analistas e investigadores, se produjeron importantes ahorros en la consolidación de sus procesos de administración de casos en una visión de la empresa. Cuando sumamos el efecto neto de los beneficios esperados mensualmente, estimamos que el sistema ahorraría casi US$90.000 por mes en mejoras por eficiencias y medidas más precisas para la detección del fraude. Cuando analizamos los resultados en el cuadro al lado izquierdo, los beneficios más importantes fueron la identificación de los nuevos riesgos de fraude y la eliminación del esfuerzo del trabajo duplicado.

El retorno de la convergencia

Las instituciones financieras están siendo impulsadas para mejorar las eficiencias y ser más efectivas para combatir los riesgos de crímenes financieros. Los criminales sofisticados y los clientes de alto riesgo disfrutan de un relativo anonimato explotando los canales impersonales y el comercio electrónico. Las agencias regulatorias, las asociaciones comerciales, las unidades de inteligencia financieras y las mejores prácticas de la industria recomiendas un enfoque holístico para dirigir las investigaciones.

Nuestro ejemplo de caso de estudio demuestra que existe un beneficio económico para justificar la inversión en un sistema de administración de casos en la empresa para integrar los procesos ALD y de fraude. Lograr una visión holística de la conducta de un sujeto en toda la empresa es un buen primer paso hacia un modelo operativo de crímenes financieros.

A medida que aumenta la adopción por parte de la industria, la integración de la información de los crímenes financieros en todos los canales será empujada hacia las funciones de detección y de administración de alertas. El uso de la tecnología para ejecutar decisiones en tiempo real en el punto de venta será crucial con la adopción de la banca móvil. La última generación de sistemas ECM brinda una base para entender los riesgos de crímenes financieros en la empresa. En efecto, "¿cuál es mi exposición a los eventos conocidos o las pérdidas?". Una vez que estas exposiciones puedan ser cuantificadas y medidas exactamente, las instituciones tendrán un mapa de ruta mucho más claro de dónde invertir los recursos que están alineados con la exposición actual al riesgo de crímenes financieros.

David Stewart, CAMS, Jefe de Industria Bancaria en la Práctica Global de Fraude y Crímenes Financieros, SAS, Cary, NC, EE.UU., David.Stewart@sas.com

Dan Barta, Examinador de Fraude Certificado y Especialista Senior en Fraude a Empresas, SAS, Dallas, TX, EE.UU., Dan.Barta@sas.com

PICs entre nosotros

Está claro que las compañías de inversión privada (PICs, por sus siglas en inglés) son uno de los vehículos de planificación financiera más analizados en la escala de riesgo antilavado de dinero. Ellos están definidos en el Manual de Examen LSB/ALD del FFIEC de los EE.UU., junto con todas las variaciones del espectro de las entidades comerciales. El manual los define, describe sus riesgos y brinda prácticas adecuadas de mitigación del riesgo. Todo es muy directo, y con políticas y procedimientos rigurosos y un estricto enfoque basado en el riesgo, las compañías deberían poder mantener los PICs bajos control. Por supuesto, eso siempre que la gente dónde están realmente en su institución. Ése es un desafío mayor.

En mi experiencia, las PICs no están alrededor de los portfolios agitando una bandera roja. Aunque se concentran principalmente en la banca privada, la verdad es que las PICs y sus variaciones esconderse en cualquier lado. Sin ninguna advertencia, pueden entrar silenciosamente en su peor escenario cuando menos lo espere — durante un examen desafiante, o incluso peor, como parte de una investigación.

Usted puede verse tentado de descartar este concepto como la falta de controles efectivos por parte de una institución y de evaluaciones del riesgo deficientes. Antes de hacerlo, considere la población de las cuentas existentes abiertas mucho antes de que fueran implementados en su institución los rigurosos procedimientos PIC, de que los portfolios que han sido heredados de fusión en fusión, migraran de a una línea de negocios a otra, o se reasignaran de un oficial a otro. Ese es solo un factor a considerar en búsqueda de PICs que no son detectadas.

Podría haber muchas causas que contribuyan al misterio. Analicemos algunos de los factores más probables:

Supuestos — La razón número uno para no detectar PICs es asumir que solo son utilizados por clientes de banca privada. El hecho de que su organización tenga un modelo de negocios que ofrece planificación offshore no garantiza que las PICs no estén siendo utilizadas por clientes fuera de su modelo de negocios definido y todos sus controles.

Cuentas Existentes — Como se indicó previamente, la población de cuentas existentes de todas las líneas de negocios representa la mayor exposición. En un mundo de fusiones, realineamientos comerciales, cambios de personal, varias tomas del control por rescate de instituciones en dificultades, es prácticamente imposible tener el control de todas las cuentas de sus portfolios.

Relaciones Existentes — Ésta es una causa más sutil pero fundamente de las PICs no detectadas. Pueden ser relaciones sólidas, conocidas de su institución que han evolucionado a lo largo de los años y se han convertido en relaciones complejas atendidas por varias líneas de negocios, pero donde el principal punto de contacto con el cliente sigue siendo el oficial que inició la relación. Estas situaciones pueden hacer que los límites se desdibujen y que los controles se debiliten. Por ejemplo, una relación comercial con cuentas personal para los dueños del negocio y sus familias. La banca privada puede atender las cuentas personales, y los productos de inversión pueden provenir del departamento de corretaje.

Sin embargo, cuando se necesite una cuenta para una nueva "entidad", la PIC puede ser parte del portfolio comercial y ser considerada como otra cuenta comercial, no necesariamente una que siga los controles adecuados. Es cierto que los procedimientos efectivos de apertura de cuentas implican que el oficial comercial identifique la naturaleza de la nueva entidad, pero ello es así cuando el factor del conocimiento entra a jugar un papel.

Conocimiento — Los banqueros privados internacionales saben qué son las PICs. Ellos conocen sus riesgos, y que deben cumplir con procedimientos estrictos. Sin embargo, lo mismo puede no ser cierto para el resto de los oficiales de su institución, incluso los banqueros privados que tratan con clientes estadounidenses. El resto de la base de empleados puede tener conocimientos muy limitados de las PICs obtenido en la capacitación ALD anual. Sin embargo, esto generalmente implica una pequeña exposición real a reconocer a las PICs cuando se abre una cuenta nueva, o identificar a las PICs remanentes en sus portfolios ya existentes. Como resultado de ello, incluso los procedimientos de cuentas nuevas pueden ser erróneamente salteados, y los controles diseñados para verificar las PICs pueden ser obviados.

Tecnología — Vivimos en un mundo de tecnología donde los sistemas mandan. Cualquier cosa y todo lo que usted siempre quiso saber sobre las cuentas de su institución está al alcance de su mano. ¿Correcto? ¡Error! Los sistemas han mejorado tremendamente, y son la mejor herramienta para mejorar los controles que van desde la apertura de cuentas hasta el monitoreo. Sin embargo, la realidad es que la mayoría de los sistemas de las instituciones, incluso de las más grandes, siguen siendo un desafío. Los identificadores de sistemas utilizados para detectar a las PICs pueden no existe, y el agregar un campo adicional para obtener esta información puede ser un esfuerzo importante. Además, aún cuando se pueda agregar el campo, hay que completarlo. Eso no incluye a los numerosos sistemas distintos utilizados para los diferentes productos y líneas de negocios, y los sistemas que todavía no están totalmente integrados años después de una fusión.

Este es un panorama aleccionador de una batalla perdida, pero no tiene porqué ser así. Por la razón indicada, existe un enfoque que puede solucionarlo. Puede requerir tiempo,

y uno debe ser creativo con los recursos que tiene, pero puede solucionarse. El resultado impactará en las cuentas existentes, y ayudará a establecer procesos más adaptados a las cuentas nuevas, a reforzar la capacitación, y mejorar la resolución de cualquier actividad anormal logrando un mejor conocimiento de la naturaleza de las cuentas. En general la mitigación del riesgo a la exposición de las PICs sería más completa.

Para evaluar la probabilidad de que existan PICs no identificadas, considere la posibilidad de realizar una revisión de cumplimiento específica. Comience por adoptar un enfoque de hallazgo. Pídale a sus recursos tecnológicos que preparen reportes utilizando campos que sean parte de la base de datos existente de la compañía, como las que puedan arrojar alguna luz sobre posibles pistas. Por ejemplo, pida un informe de las cuentas comerciales por país utilizando el campo de la dirección. Si quiere ser más específico, prepare un informe utilizando el mismo campo, pero filtre la búsqueda según las jurisdicciones offshore designadas como de alto riesgo como las designadas como tal por el GAFI, pero no se olvide de estados como Delaware. Luego diríjase a la unidad de negocios y haga preguntas.

Revise las cuentas que puedan estar ubicadas en jurisdicciones utilizadas para estructuras offshore. Identifique si las entidades son PICs realmente, y si es así, asegúrese que estén clasificadas y que se hayan aplicado los controles correspondientes. Entreviste a los oficiales responsables de las cuentas. Evalúe su conocimiento y concientización de las PICs.

Además, sea muy cuidadoso con el vocabulario utilizado para referirse a las PICs. Cualquiera sea el nombre que se use, sigue siendo una PIC. Estas pocas medidas le darán una buena idea acerca de si tiene un problema. Pueden dar lugar a un esfuerzo más estructura para eliminar portfolios de las PICs.

Siempre que tenga el tiempo y los recursos, tenga en cuenta al único factor que le asegurará el éxito a corto y largo plazo antes de embarcarse en este ejercicio. Eduque a sus oficiales y equipos de servicios y vuelva a los puntos básicos. Enséñeles no solo la definición de PIC, sino también porqué es tan fundamental saber dónde está y aplicar los controles adecuados. Déles a los empleados escenarios de la vida real. Llame a las PICs por todos los nombres que pueda imaginas para que a nadie se le pase por alto una entidad porque no tiene un signo que indique que es una PIC.

Nunca será perfecto o infalible, pero la implementación de estas sugerencias creará un escenario mucho mejor. Por supuestos, una vez que encuentre a sus PICs ocultas, tendrá que hacer algo con ellas, pero ése es otro tema.

La siguiente es la pregunta eternal de la evaluación del riesgo:

¿Se siente más cómodo al conocer el riesgo o es mejor no saberlo?

En mi opinión, es mejor saber y seguir un enfoque realista basado en el riesgo para mitigar el riesgo. Créanme, las noches sin dormir por no saber son mucho peores.

M. Carolina Rivas Liendo, CAMS, Engaged AML Solutions, Inc., Florida, EE.UU., carolinarl@engagedaml.com

India – Comprometida a combatir el lavado de dinero

India, que ingresó al GAFI en junio de 2010 como su miembro número 34, ha asumido varios esfuerzos para mejorar su régimen antilavado de dinero (ALD). Dentro del contexto de la reunión del Grupo Asia/Pacífico sobre Lavado de Dinero (APG, por sus siglas en inglés)[1] realizada en julio de 2011, el Ministro de Finanzas indio Pranab Mukherjee fue citado al destacar el compromiso de su país para enfrentar al lavado de dinero y el financiamiento del terrorismo. El señor Mukherjee dijo que se habían implementado varias medidas para mejorar el régimen ALD/CFT, a tono con los estándares del GAFI, como se informó en *The Hindu* el 23 de julio de 2011.[2] India ha triplicado recientemente la cantidad de personal de la Dirección de Control Legal, que dirige las investigaciones de lavado de dinero en el país. India también ha creado recientemente una Unidad de Inteligencia Financiera, que incluye un sistema de reporte de operaciones financieras sospechosas, recordó Mukherjee.[3] El país, sin embargo, sigue enfrentando varios desafíos. Estos desafíos están indicados aquí y puestos aquí en el contexto del régimen ALD y otros esfuerzos asumidos en apoyo de la estructura actual.

Una montaña a escalar — corrupción, lavado de dinero y terrorismo

India, que a menudo es elogiada por ser una de las democracias más antiguas y más grandes del mundo, desde comienzos de 2011, ha recibido importantes críticas en los medios internacionales y locales en relación con la corrupción generalizada, que ha impregnado a todos los niveles de la sociedad, el gobierno y los negocios. Según el Barómetro de Corrupción Global de Transparencia Internacional de 2010, India es el tercer país más grande de la región Asia/Pacífico después de Camboya y Afganistán.

Como resultado de los escándalos de corrupción, el lavado de dinero se ha convertido en un tema político en India, con la oposición acusando al gobierno de no hacer lo suficiente para devolver los fondos ilegales que han sido transferidos al exterior.[4] De acuerdo con otras fuentes periodísticas, unos US$ 450.000 millones de fondos ilegales o ganancias no gravadas obtenidas en India han sido depositados en bancos extranjeros.[5] Las fuentes citadas en el periódico indio *Economic Times* sugieren que, según estimaciones extraoficiales, esa suma podría llegar al US$ 1,4 billón. Se estima que Mauricio es uno de los mayores inversores extranjeros en India.[6] Esto es alarmante dado que los fondos invertidos en India procedentes de Mauricio son considerados en gran medida fondos lavados. Según un artículo publicado en el *Economic Times*,[7] India planea hacer amplias reformas a las regulaciones sobre impuestos directos e indirectos. Es de particular interés que los planes del nuevo régimen impositivo incluyan a todas las ganancias pasivas obtenidas por residentes titulares de tenencias accionarias importantes en compañías constituidas en jurisdicciones de baja tributación fiscal a fin de eludir las actividades de lavado de dinero. El mismo artículo destacaba que es poco probable que el nuevo régimen sea presentado pronto debido a las desavenencias entre el gobierno federal y los estados gobernados por la oposición. India sin embargo, ha sufrido varios ataques terroristas importantes, el más reciente en julio de 2011 en la capital comercial de India, Mumbai, recordándole a la nación la amenaza terrorista que enfrenta y la importancia de las medidas ALD y CFT.

El *Informe de Evaluación Mutua de India* elaborado por el GAFI, publicado en junio de 2010, señalaba que las principales fuente de lavado de dinero en India eran consecuencia de una serie de actividades ilegales cometidas dentro y fuera del país, principalmente el tráfico de drogas, el fraude, la falsificación de la moneda de India, el crimen organizado transnacional, el tráfico humano y la corrupción. La amenaza de lavado de dinero en India también proviene de sus regiones fronterizas y por lo tanto también debería ser considerada en este contexto. Según una declaración publicada por el GAFI en junio de 2011, Sri Lanka se encuentra entre las jurisdicciones con importantes deficiencias ALD/CFT. Estos países no han hecho progresos suficientes para solucionar las deficiencias o no han comprometido un plan de acción elaborado con el GAFI para resolver las deficiencias.[8] Además, Nepal y Pakistán también estaban en la lista elaborada por el GAFI como países cuya mejora en el cumplimiento ALD/CFT está en un proceso constante.[9]

Métodos de LD en India

De acuerdo con el *Informe de Evaluación Mutua de India* preparado por el GAFI, los métodos más comunes de lavado de dinero utilizados en los delitos locales son la apertura de múltiples cuentas bancarias, la mezcla de fondos ilegales con bienes de origen legal, la compra de cheques bancarios con efectivo y el recorrido y dirección del mismo a través de complejas estructuras legales. Para los crímenes organizados transnacionales, el informe señala que el origen

[1] Una organización internacional autónoma y de cooperación, cuyos miembros son 40 países y otros observadores internacionales y regionales. http://www.apgml.org/
[2] http://www.thehindu.com/news/national/article2285886.ece
[3] http://articles.timesofindia.indiatimes.com/2011-07-19/india/29790686_1_money-laundering-act-financial-action-task-force-laundering-and-terror-funding
[4] http://www.business-standard.com/india/news/us-offers-assistance-in-dealingmoney-laundering/136736/on
[5] http://www.economist.com/node/18338852
[6] Según el Dr. Christoph Hein, Corresponsal Asia-Pacífico del importante diario de Alemania *Frankfurter Allgemeine Zeitung:* http://www.faz.net/artikel/C30974/keine-fragen-keine-namen-keine-quittung-30347540.html
[7] http://articles.economictimes.indiatimes.com/2011-06-20/news/29679834_1_indirect-tax-tax-regime-tax-evasion
[8] http://www.fatf-gafi.org/document/54/0,3746,en_32250379_32236992_48263734_1_1_1_1,00.html - srilanka
[9] http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32236992_48263965_1_1_1_1,00.html

criminal de los fondos es ocultado utilizando compañías offshore y técnicas de lavado de dinero basadas en el comercio.

El periódico *The Hindu* informaba que una de las principales áreas analizadas en el 14ta. reunión anual del Grupo Asia/Pacífico sobre Lavado de Dinero, realizada en julio de 2011 estaba referida al fondeo del terrorismo y el uso de redes de telemercadeo para cometer delitos transnacionales, además de lavado de dinero.[10]

Régimen ALD de India

Como se indicaba en el *Informe de Evaluación Mutua de India*, publicado por el GAFI en junio de 2010, el régimen ALD/CFT de India es relativamente nuevo. Desde 2005, la Ley de Prevención del Lavado de Dinero (PMLA, por sus siglas en inglés) ha sido aplicada y fue modificada más recientemente en 2009. La Ley de (Prevención) de Actividades Ilegales (UAPA, por sus siglas en inglés) que penaliza al financiamiento del terrorismo, ha sido aplicada desde 1967. Fue modificada más recientemente en 2008 para colocar a la ley más en línea con las obligaciones de la Convención de la ONU para la Supresión del Financiamiento del Terrorismo.

Aunque el informe elogia a la India por su mayor atención al lavado de dinero y su serio compromiso frente al combate al terrorismo, el informe critica la falta de condenas por lavado de dinero o actividades terroristas y la falta de sanciones efectivas, disuasivas o proporcionales por las deficiencias ALD/CFT. En este aspecto el informe destaca que los casinos son los únicos Negocios y Profesiones No Financieros Designados (DNFBP, por sus siglas en inglés), incluidos en el PMLA.

El Informe de Evaluación Mutua hace una serie de recomendaciones a fin de mejorar el régimen ALD/CFT de la India:

- Corregir las deficiencias técnicas en la penalización del lavado de dinero y del financiamiento del terrorismo y en el marco local de la confiscación y las medidas provisorias
- Ampliar las obligaciones de diligencia debida sobre el cliente con medidas claras y específicas para mejorar las obligaciones actuales con relación a la propiedad beneficiaria
- Mejorar la fiabilidad de los documentos de identificación, el uso de cuentas comunes *(pooled accounts)*, PEPs, y los negocios que no son realizados en forma personal
- Lograr que el Correo de India, que recientemente fue incluido como sujeto a la PMLA, implemente efectivamente las obligaciones ALD/CFT
- Mejorar la efectividad del régimen supervisor del sector financiero y asegurar que el Correo de la India[11] esté supervisado adecuadamente
- Asegurar que los integrantes de las autoridades supervisoras realicen modificaciones a sus regímenes de sanción para permitir sanciones efectivas, proporcionales y disuasivas por omisiones en el cumplimiento de las obligaciones ALD/CFT
- Ampliar las obligaciones PML a todo el espectro de las DNFBPs, y asegurar que sean efectivamente reguladas y supervisadas.

Ya desde la publicación de este informe, India parece haber continuado trabajando para mejorar su régimen de lavado de dinero.

En julio de 2011 el *Indo Asian News Service*[12] informó que la Suprema Corte de India había formado un Equipo de Investigaciones Especiales (SIT, por sus siglas en inglés) para investigar los incidentes de lavado de dinero, especialmente la evasión fiscal. El comité es presidido por el ex juez de la Suprema Corte, B.P. Jeevan Reddy.[13]

Además, en mayo de 2011, el periódico indio *Business Standard* informó que los EE.UU. habían ofrecido asistencia a la India para apoyar los esfuerzos del país para combatir el lavado de dinero y el terrorismo.[14] Los dos países acordaron continuar la cooperación entre las agencias aduaneras de India y los EE.UU. y explorar nuevas áreas de interés mutuo para proteger la seguridad de la cadena de suministros global.

La amenaza del terrorismo

Los expertos indican que India enfrenta serias amenazas de docenas de grupos extremistas. Según un artículo publicado en *The Times Of India* el 12 de agosto de 2008, unas 800 células terroristas actúan en la India. Según un extenso informe sobre *Grupos Terroristas en la India (Terrorist Groups in India)* publicado por el Consejo de Relaciones Exteriores, es difícil determinar la cantidad exacta de grupos que orquestan ataques en la India debido a los movimientos separatistas.[15] El Portal *South Asia Terrorism*, un proyecto del Instituto para la Administración del Conflicto, un grupo pensador independiente ubicado en Nueva Delhi, incluye a una gran variedad de grupos terroristas organizados en toda India.[16] India ha sufrido varios ataques terroristas importantes, el más reciente el 13 de julio de 2011 en Mumbai, una ciudad que ha sido el blanco más preferido de la mayoría de las organizaciones terroristas, principalmente las fuerzas separatistas de Pakistán. De acuerdo con la información publicada en *Wikipedia*, Mumbai es la ciudad más rica de India y tiene el PBI más elevado de todas las ciudades del sur, oeste o centro de Asia.[17] La publicación *The Economist* informó el 13 de julio de 2011, que la inteligencia india tema que jóvenes musulmanes en el país esté creciendo con una característica más radical y están aquellos convertidos al radicalismo que trabajan como obreros migrantes en los países de la región del Golfo. Con relación a los ataques de 2011, algunos sospechas que los Mujahideen indios, podrían tener vinculaciones con los jihadistas pakistaníes como los Lashkar-e-Tayyaba.[18]

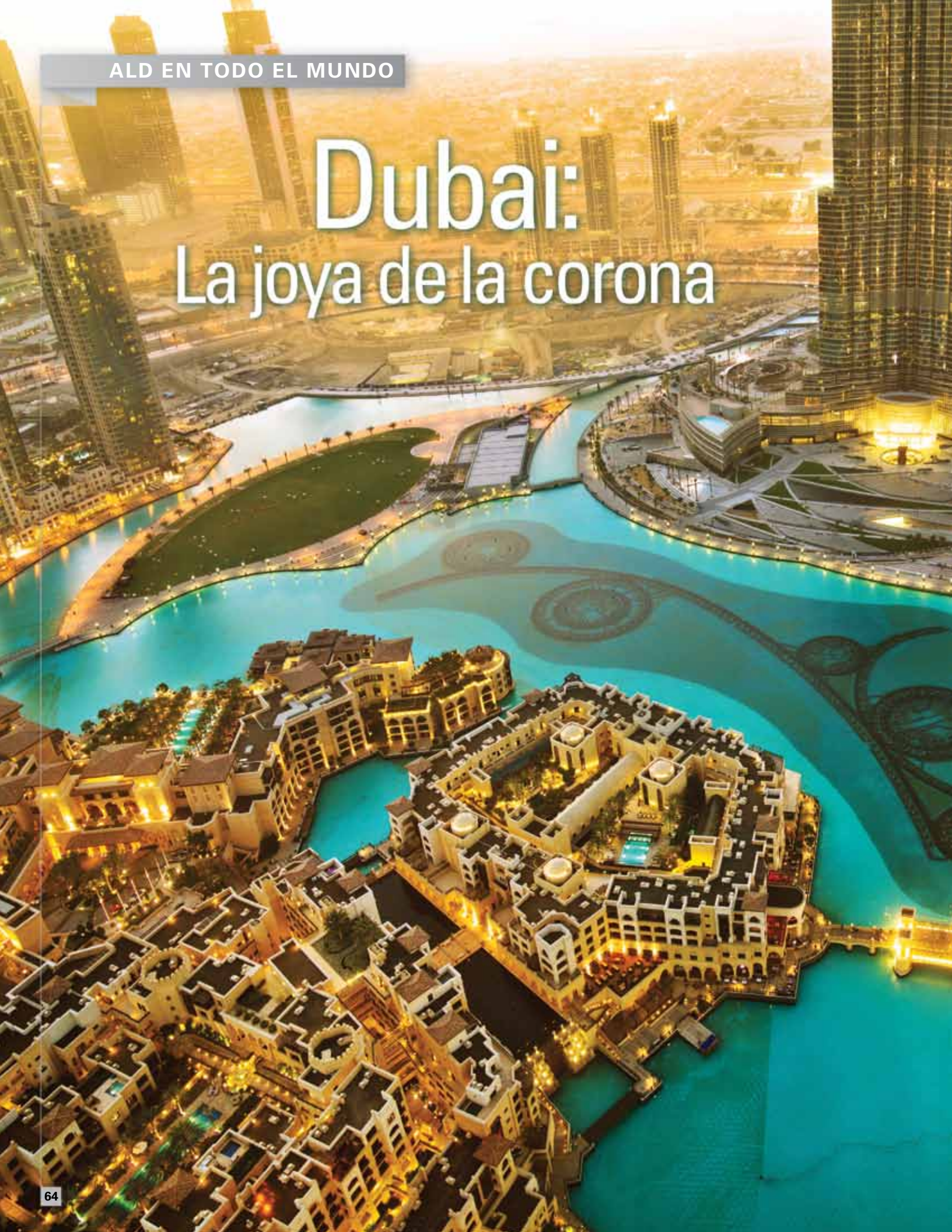
Conclusión

Dado el tamaño de la economía India y su geoestratégica ubicación, tiene un rol importante que jugar en el combate del lavado de dinero y del financiamiento del terrorismo. Parece estar acercándose al desafío y comprometida con su obligación de trabajar con socios experimentados para llegar a dominar la enorme tarea que enfrenta.

Jennifer Hanley-Giersch, CAMS, directora administradora, Business Risk Research Limited, Berlín, jennifer.hanley business-risk-research.com

[10]http://www.thehindu.com/news/national/article2285886.ece
[11]http://www.indiapost.gov.in/NSDefault.htm & http://en.wikipedia.org/wiki/Indian_Postal_Service
[12]http://in.news.yahoo.com/apex-court-appoints-probe-team-money-laundering-142950379.html
[13]Otros miembros incluyen al vicegobernador del Banco de la Reserva de la India, al director de la Oficina de Inteligencia de la India, la Dirección de Control Legal y la Oficina Central de Investigaciones, al Presidente y el Secretario conjunto de la Junta Central de Impuestos Directos, al director general de la Oficina de Control de Narcóticos e Inteligencia de Ingresos y al director de la UIF.
[14]http://www.business-standard.com/india/news/us-offers-assistance-in-dealingmoney-laundering/136736/on
[15]http://www.cfr.org/india/terror-groups-india/p12773
[16]http://www.satp.org/satporgtp/countries/india/terroristoutfits/index.html
[17]http://en.wikipedia.org/wiki/Mumbai
[18]http://www.economist.com/blogs/banyan/2011/07/bombs-mumbai

Dubai:
La joya de la corona



Para cualquiera que quiera hacer negocios en el Medio Oriente, el primer puerto de escala es el pequeño pero estratégicamente ubicado Emirato de Dubai, enclavado en el impresionante desierto de la Península Árabe y sobre el prístino Golfo Pérsico. Su opulencia y sofisticación es reconocida mundialmente, es el hogar del edificio más alto del mundo, el rascacielos Burj Khalifa. También alberga a uno de los hoteles más caros del mundo, el Burj al-Arab, y al moderno Centro Financiero Internacional de Dubai (DIFC, por sus siglas en inglés).

Dubai está en el mismo centro del sistema financiero del Medio Oriente, tanto el legítimo como el ilegítimo. Es la puerta de ingreso del US$1,2 billón de la industria financiera islámica que se estima crecerá hasta alcanzar los US$4 billones en los próximos años[1], igual que el multimillonario comercio del opio afgano[2].

Dubai: El corazón del Golfo Pérsico y el petrodólar

La Agencia Internacional de Energía en su Informe de Energía Mundial de 2009, estimó que entre 2008 y 2030, los ingresos de la OPEC por el petróleo llegarían a los US$23 billones[3].

Según José Franco del *Khaleej Times*, los balances consolidados de los bancos árabes totalizaron US$2 billones en 2007[4]. Se espera que los bienes extranjeros netos de los países del Consejo de Cooperación del Golfo (GCC, por sus siglas en inglés) se incrementen de US$1,049 billones a fines de 2009 a US$1,34 billones a fines de 2011, o el equivalente al 122% del PBI de la región[5]. Mientras tanto, según Invesco, los Fondos de Riqueza Soberana de la región del Golfo — que alcanzan al 44% de los flujos globales SW, y que representan algo más de US$1 billón — están disminuyendo desde el exterior y aumentando a inversiones

[1] Mushtak Parker, *El Banco Mundial Declara Área de Prioridad a las Finanzas Islámicas (World Bank Declares Islamic Finance a Priority Area)*, Arab News, May 16, 2011, http://arabnews.com/economy/islamic-finance/article405986.ece

[2] *ADICCIÓN, CRIMEN E INSURGENCIA: La amenaza transnacional del opio afgano, Oficina de las Naciones Unidas sobre Narcóticos y Crímenes (ADDICTION, CRIME AND INSURGENCY: The transnational threat of Afghan opium*, United Nations Office on Drugs and Crime) (UNODC), October 2009, http://www.unodc.org/documents/data-and-analysis/Afghanistan/Afghan_Opium_Trade_2009_web.pdf

[3] IEA Panorama Mundial de la Energía, 2009 (*2009 World Energy Outlook*, IEA), 125, http://www.iea.org/textbase/nppdf/free/2009/WEO2009.pdf

[4] *Jose Franco, Balances de los bancos árabes llegan a los US$2 billones* (José Franco, Arab banks balance sheet to reach $2tr), Khaleej Times, December 13, 2007, http://www.khaleejtimes.com/DisplayArticleNew.asp?xfile=data/business/2007/December/business_December344.xml&section=business&col=

[5] *Isaac John, activos extranjeros netos del Consejo de Cooperación del Golfo alcanzan los US$1, 34 billones en 2011 (GCC net foreign assets to hit $1.34tr in 2011): IIF*, Khaleej Times, November 5, 2010, http://www.khaleejtimes.com/DisplayArticle09.asp?xfile=data/business/2010/November/business_November138.xml&section=business

locales a la luz de la "primavera árabe"[6]. Se espera que solo el GCC invierta US$3 billones en proyectos de infraestructura para fines de 2020[7]. En consecuencia, el Medio Oriente en general, y Dubai en particular, se ha convertido en un imán para los "financistas" de todo el mundo que desean aprovechar el aumento inexorable del petrodólar.

En 2009, la reconocida revista *The Banker* estimaba que 48 países, 628 instituciones inscriptas y 435 instituciones cumplidoras de la shariah, conformaban el US$1 trillón de la industria financiera islámica.[8] Según la Cámara de Comercio e Industria de Dubai, los bancos islámicos de los Emiratos Árabes Unidos (EAU), la segunda economía árabe más grande la zona, continuaban su crecimiento firme en 2010, con los activos de los bancos incrementándose en alrededor de un 11 por ciento.

A fines de 2010, los Emiratos Árabes Unidos tenían ocho bancos islámicos, con cerca de 260 sucursales, controlando alrededor de US$54.000 millones en depósitos. Tenían alrededor del 10,9 por ciento del total de los depósitos con los 23 bancos nacionales y las 28 unidades extranjeras del país.[9] En resumen, las finanzas islámicas son enormes y continúan aumentando.

Por otro lado, en 2009, en términos de activos, con US$293.200 millones, Irán, seguido de Arabia Saudita (US$127.900 millones), tenía la mayor cantidad de activos de conformidad con la shariah. Los bancos iraníes tenían alrededor del 40 por ciento de los activos totales de los 100 principales bancos iraníes del mundo, y el más importante era el Bank Melli Iran, que había sido sancionado por la OFAC, con activos por US$45.500 millones, ocupaba el primer lugar. Otros bancos iraníes sancionados ocupaban lugares próximos en la lista: el Bank Mellat con US$39.700 millones y el Bank Saderat Iran con US$39.300 millones. De hecho, 6 de cada 10 de los principales bancos islámicos son iraníes.[10] En consecuencia, los bancos occidentales tienen que ser cuidados respecto de con quién están haciendo negocios, y reconocer que actualmente Irán es la base fundamental de las finanzas islámicas.

El cuasi colapso del proyecto estatal Dubai World a fines de 2009 expuso penosamente los peligros de la industria financiera islámica subdesarrollada y escasamente regulada. Su fallido bono islámico Nakheel (sukuk) emitido por US$4.100 millones y el hecho de soportar la carga de una deuda de US$10.900 millones[11] utilizados para pagar la construcción del ambicioso proyecto Palms, que está formado por espectaculares propiedades ejecutivas sobre terreno ganado al mar,[12] precipitaron la caída del mercado inmobiliario.[13] Esto estuvo lejos de lo que fue el lanzamiento en noviembre de 2006 del sukuk Nahkeel por US$2.500 millones. Sus arquitectos declararon que el sukuk cumpliría con los principios islámicos de la Sharia, y estaría basado en el principio islámico del Ijara (leasing financiero). En declaraciones formuladas a la prensa en esa época, el Dubai World garantizaba las obligaciones de pago bajo el Sukuk. El Dr. Mohamed Khalfan bin Kharbash, Ministro de Estado de Finanzas e Industria de los Emiratos Árabes Unidos y Presidente de DIB, dijo: "Esta transacción histórica del proyecto Dubai World y el Grupo Nakheel marcará nuevos puntos de referencia en la industria financiera … El primer Sukuk de su tipo vinculado a estructuras de activos hace que sea una transacción atractiva para una amplia variedad de inversores".[14] No pudo ser; los inversores occidentales aprendieron a su pesar muchas de las debilidades de las finanzas islámicas, incluida su falta de transparencia y responsabilidad, así también como su falla en la protección efectiva de los acreedores, muchos de los cuales se encontraron sin recursos, y otros solo conservaron la esperanza de obtener algunos centavos sobre los dólares que habían invertido en éste que alguna vez fue considerado un sukuk heráldico.

Tráfico de drogas y narcoterrorismo afgano

Afganistán provee más del 90 por ciento de la oferta global de los opiáceos ilegales (opio, heroína y morfina). El valor del mercado global de opiáceos se estima en US$65.000 millones. Solo un 5-10% (US$3.000-US$5.000 millones) de estos fondos ilícitos es lavado a través de actividades legales de comercio y el sistema bancario convencional.[15]

En 2006-2007, los fondos vinculados con el tráfico de drogas destinados a los insurgentes afganos y los líderes militares fueron estimados por la UNODC entre US$200 y US$400 millones anuales.[16] Las exportaciones de opiáceos de Afganistán se han modificado y ahora integran una mayor porción de productos refinados. Esto le ha permitido al grupo Talibán aplicar impuestos a productos de mayor valor agregado (productos refinados) y otras actividades vinculadas con las drogas: procesamientos en laboratorio, tráfico e importaciones de productos precursores — un negocio de alrededor de US$3.000 millones en 2007 solo en Afganistán.

Además, el Talibán y otros grupos vinculados a Al Qaeda han estado recibiendo una participación cada vez mayor de los US$1.000 millones que se mueven en el mercado del opio en Pakistán.[17] En Pakistán, los Shinwaris, la segunda tribu más grande de Khyber, son dueños de importantes compañías logísticas, algunas con oficinas en puertos paquistaníes y también en Dubai.[18] Los miembros de la gran diáspora afgana en Dubai ayudan a los comerciantes, tanto para el tráfico en pequeña escala como para los grandes movimientos

[6] Isaac John, *Gulf SWFs to focus on local investments*, Khaleej Times, May 24, 2011, http://www.khaleejtimes.com/biz/inside.asp?xfile=/data/business/2011/May/business_May448.xml&section=business

[7] Muzaffar Rizvi, *GCC to invest $3tr in Infrastructure*, Khaleej Times, December 26, 2010, http://www.khaleejtimes.com/biz/inside.asp?xfile=/data/business/2010/December/business_December453.xml&section=business

[8] *Las 500 Instituciones Financieras Más Importantes (Top 500 Islamic Financial Institutions)*, The Banker, November 2009 Supplement, 2 http://www.mifc.com/index.php?ch=151&pg=735&ac=395&bb=657

[9] Shveta Pathak, *UAE Islamic Banks' Assets Grow 11 p.c.*, Arabian Gazette, July 3, 2011, http://arabiangazette.com/uae-islamic-banks-assets-grow-11-p-c/

[10] *Bank Melli Iran, the largest Islamic bank*, PressTV, August 28, 2009, http://edition.presstv.ir/detail/104662.html; Top 500 Islamic Financial Institutions, 4

[11] Shaheen Pasha and Rachna Uppal, *Nakheel Seen Offering Sukuk to Trade Creditors*, Reuters, March 28, 2010, http://www.reuters.com/article/2010/03/28/us-nakheel-sukuk-idUSTRE62R0SA20100328; Shaheen Pasha, Planned Nakheel Sukuk on Offer at 20 pct Discount, Reuters, June 9, 2011, http://www.reuters.com/article/2011/06/09/nakheel-sukuk-idUSLDE75815L20110609

[12] Shane McGinley, *Nakheel to Issue Sukuk by January 2011 — CEO*, Arabian Business.com, October 18, 2010, http://www.arabianbusiness.com/nakheel-issue-sukuk-by-january-2011-ceo-357102.html

[13] *Problemas de la Deuda de Dubai Exponen el Modelo de Gobierno (Dubai's Debt Woes Expose Governance Model)*, The International Institute For Strategic Studies, Volume 16, Comment 9, March 2010, http://www.iiss.org/EasysiteWeb/getresource.axd?AssetID=37791&type=full&servicetype=Attachment; IMF Country Report No. 10/42, February 2010, 4, 11-13, 14 http://www.imf.org/external/pubs/ft/scr/2010/cr1042.pdf

[14] Grupo Nakheel Emite Deuda Sukuk por US$2.500 millones (Nakheel Group Launches USD 2.5 Billion Sukuk), November 7, 2006, http://www.ameinfo.com/101035.html

[15] ADDICTION, CRIME AND INSURGENCY, 7

[16] ADDICTION, CRIME AND INSURGENCY, 2

[17] ADDICTION, CRIME AND INSURGENCY, 3

[18] ADDICTION, CRIME AND INSURGENCY, 125

financieros.[19] Esta realidad debería hacer que las instituciones financieras occidentales estén atentas cuando realizar operaciones con esta importante pero peligrosa zona del mundo.

Según Juan Miguel del Cid Gómez, al-Barakaat, una red de empresas, incluidas compañías de telecomunicaciones y construcción, así como también de remesas de dinero y servicios de cambio de dinero en efectivo de los Estados Unidos y Somalia, fue una parte integral de los primeros esfuerzos de recaudación de fondos de Al Qaeda. Al-Barakaat administró, invirtió y distribuyó fondos para *Al Qaeda.* La mayoría de las transacciones de Bin Laden fueron realizadas entre Mogadishu (Somalia), Dubai (EAU) y Mombasa y Nairobi (Kenia). Además, Gómez señala que muchas transacciones de hawala se originan en, o están destinadas a Dubai o Yemen. Finalmente, señala que uno de los patrocinadores de los ataques del 11/9, Khalid Sheikh Mohamed, envió una importante suma de dinero (posiblemente unos US$200.000) a Abdul Aziz Ali en Dubai, quien posteriormente la transfirió a los secuestradores en los EE.UU.[20]

Cables de la diplomacia estadounidense publicados por Wikileaks subrayaban la vulnerabilidad de los EAU en general, y de Dubai en particular, al lavado de dinero y el financiamiento del terrorismo: "El punto puede enfatizarse en que el rol de los EAU como centro financiero global cada vez más importante, junto con al supervisión regulatoria deficiente, hace que sea vulnerable al abuso de los financistas del terrorismo y las redes de facilitación", indicaba un cable del Departamento de Estado. En otro cable de diciembre de 2009, Howard Mendelsohn, a cargo de la Secretaría Asistente de la Oficina de Inteligencia y Análisis del Departamento del Tesoro de los EE.UU., indicaba que el "se cree que el Talibán y la Red Haqqani [un grupo con sede en Pakistán que lucha contra las fuerzas de la OTÁN en Afganistán] reciben dinero proveniente de sus negocios con sede en los EAU".[21]

En diciembre de 2010, dos hermanos paquistaníes, afirmaron estar en contacto con el entonces número tres de la organización Al Qaeda, Abu al-Yazid, juzgado en los EAU. Los dos empresarios fueron acusados de entregar laptops, telescopios, linternas muy finas especiales y cuchillos suizos a Waziristán, un semillero de Al Qaeda, el Talibán y otros grupos radicales islámicos.[22]

Más recientemente, el *Wall Street Journal* informó que Ousama Abushagur, un ejecutivo de telecomunicaciones libio de 31 años criado en Huntsville, Alabama, planificó una operación de asistencia a los rebeldes desde su cada en Abu Dhabi. Abushagur y dos amigos de la infancia que trabajan como gerentes de empresa en Dubai y Doha comenzaron a recaudar fondos el 17 de febrero de 2011, para apoyar las protestas políticas que surgían en Libia. El 23 de febrero, cuando la lucha ya se había iniciado, su equipo envió el primero de varios convoyes con ayuda humanitaria al este de Libia.[23]

Un centro global de lavado de dinero

Naresh Kumar Jain es un multimillonario indio sobre el que se sospecha que es uno de los lavadores de dinero más importantes del mundo. Los investigadores creen que sus negocios se apoyan en grandes sumas de dinero en efectivo proveniente de África y que él recibe de contrabandistas de diamantes y traficantes de drogas, la mayoría del cual llega a Dubai en valijas. Por su parte, los grupos de piratas organizados que operan en Dubai y otros estados del Golfo están lavando grandes sumas de dinero recibido de los rescates pagados por los secuestros de buques en las afueras del Cuerno de África. Según un artículo publicado por el periódico *British Observer* en diciembre de 2009, el entonces embajador estadounidense en Afganistán, E. Anthony Wayne, indicó que cada día se contrabandean US$10 millones en efectivo desde Kabul a Dubai, y son transportados en valijas. Wayne indicó que una investigación realizada por los EE.UU. descubrió que US$190 millones en efectivo fueron contrabandeados en solo 18 días.

Nick Mathiason de la Fundación Fairtrade y que previamente había sido corresponsal de negocios de los diarios *The Guardian* y *The Observer* durante 10 años fue citado en un artículo de enero de 2010 publicado en *The Observer:* "Fuentes internas dicen que obtener un pasaporte de los EAU, que permite a su titular abrir una cuenta bancaria, todavía es relativamente fácil. Los expertos sugieren que las aduanas de los aeropuertos en algunos de los estados de los EAU facilitan las rutas para trasladar artículos y dinero en efectivo. Además, la propiedad inmobiliaria en Dubai tiene una reputación notoria de ser utilizada para lavar dinero, ya que los departamentos son adquiridos por entidades desconocidas y nadie vive nunca allí".[24]

No debería sorprender que la OFAC en febrero de 2011 haya incluido a tres compañías de Dubai — Al Adal Exchange, Green Leaf General Trading y Connect Telecom General Trading — en su Lista de Nacionales Especialmente Designados. Las empresas fueron acusadas de ser afiliadas de una importante organización de lavado de dinero proveniente del tráfico de droga en Afganistán denominada *"New Ansari Money Exchange"*. Según funcionarios de la OFAC, New Ansari ayudó a lavar dinero de dos "importantes" traficantes: un hombre llamado Haji Azizullah Alizai y la Organización Haji Juma Khan. Entre diciembre de 2009 y enero de 2010, New Ansari Money Exchange envió US$94 millones desde Afganistán a Dubai, dijeron funcionarios de la OFAC.[25]

Dubai por lo tanto representa al mismo tiempo no solo una gran oportunidad sino también un gran peligro para los negocios y bancos occidentales, ¡a riesgo del comprador!

John Wood, IPSA, consultor, Atlanta, Georgia, EE.UU., johnplayfairwood@comcast.net

[19] ADDICTION, CRIME AND INSURGENCY, 104

[20] Juan Miguel del Cid Gómez, *Un Perfil Financiero del Terrorismo de Al Qaeda y sus Afiliadas*, *Perspectivas sobre el Terrorismo (A Financial Profile of the Terrorism of Al Qaeda and its Affiliates*, *Perspectives on Terrorism)*, Vol. 4, No. 4, 2010, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/113/html

[21] Cable 10RIYADH61, http://www.wikileaks.de/cable/2010/01/10RIYADH61.html; Saudi Arabia and other Gulf states fund al-Qaeda and Taliban, Al Jazeera, December 6, 2010, http://www.rawa.org/temp/runews/2010/12/06/saudi-arabia-and-other-gulf-states-fund-al-qaeda-and-taliban.phtml

[22] *Dos Paquistaníes llevados a juicio en corte de EAU por vínculos con Al Qaeda (Two Pakistanis hauled up in UAE court for links with Al Qaeda)*, Dubai, PTI, December 28, 2010, http://www.dnaindia.com/world/report_two-pakistanis-hauled-up-in-uae-court-for-links-with-al-qaeda_1487266

[23] Margaret Coker and Charles Levinson, *Rebels Hijack Gadhafi's Phone Network*, Wall Street Journal, April 13, 2011, http://online.wsj.com/article/SB10001424052748703841904576256512991215284.html

[24] Nick Mathiason, *Dubai's Dark Side Targeted by International Finance Police*, The Observer, January 24, 2010, http://www.guardian.co.uk/business/2010/jan/24/dubai-crime-money-laundering-terrorism; Kim Sengupta and Daniel Howden, *Pirates The $80m Gulf Connection*, The Independent, April 21, 2009, http://www.independent.co.uk/news/world/africa/pirates-the-80m-gulf-connection-1671657.html

[25] Carol Huang, *US Treasury puts Three Dubai Firms on Blacklist*, The National, March 16, 2011, http://www.thenational.ae/news/uae-news/us-treasury-puts-three-dubai-firms-on-blacklist.

Analizando el impacto de las reglas de FinCEN para los NSMs extranjeros

El 19 de julio de 2011, la Red de Control de Crímenes Financieros del Departamento del Tesoro de los EE.UU. (FinCEN, por sus siglas en inglés) publicó una regla final aclarando la definición de Negocio de Servicios Monetario (NSM) y aplicando las regulaciones de la Ley de Secreto Bancario (LSB) a las entidades extranjeras que realizan operaciones comerciales en los Estados Unidos. De acuerdo con la regla, un NSM debe cumplir con las regulaciones antilavado de dinero de la LSB si realizar transacciones por valor de US$1,000 por persona por día. Ese monto mínimo se aplica a todas las categorías de NSMs excepto a las remesadoras de dinero, que están sujetas a las reglas de la LSB, si realizan remesas de dinero por cualquier monto. La regla también reemplaza el término "corredor de divisa extranjera " por el nuevo término "corredor de divisa o cambiador", un término utilizado para incluir el cambio de instrumentos que no sean divisas como una categoría de NSM. Estas disposiciones de la regla amplían en gran medida las regulaciones y obligaciones aplicadas sobre los NSMs extranjeros.

Niveles del campo de juego

Ya no importa si la entidad es extranjera o local, inscripta o si no está autorizada o incluso si se considera a sí misma un negocio. Si la organización cumple con la definición de NSM incluida en la nueva regla está sujeta a la LSB y a otras regulaciones antilavado de dinero (ALD).

"Si una persona está sujeta a una regulación como NSM no depende de factores como ser si la persona está autorizada como negocio, si tiene empleados, o si actúa en una actividad

para obtener un lucro", según indicó FinCEN al publicar la regla. "Esta regla aclara que son las actividades realizadas las que hacen que una persona sea categorizada como un NSM sujeto a las reglas antilavado de dinero".

La regla también amplía el alcance de aquellos incluidos en las leyes LSB y ALD a las entidades que proveen servicios monetarios a los Estados Unidos aún cuando operen solo en el mundo virtual. "Una entidad califica como NSM de acuerdo con su actividad dentro de los Estados Unidos, no la presencia física de uno o más de sus agentes, agencias, sucursales u oficinas en los Estados Unidos", de acuerdo con un comunicado emitido por FinCEN. "Esta obligación surge del reconocimiento de que Internet y otros avances tecnológicos hacen que sea cada vez más posible que las personas ofrezcan servicios de NSM en los Estados Unidos desde localidades extranjeras. FinCEN busca asegurar que las reglas de la LSB se apliquen a todas las personas que realicen las actividades indicadas dentro de los Estados Unidos, sin perjuicio de su ubicación física".

Además de cumplir con todas las obligaciones reseñadas en la LSB, los NSMs extranjeros que realicen operaciones comerciales en los Estados Unidos deben designar a un agente con sede en los EE.UU. que sirva como punto de contacto con los agentes de control legal y regulatorios. Además, el agente en los EE.UU. es responsable de mantener las listas de clientes y de los datos de las transacciones.

"La regla da sustancia a la forma" dijo, vicepresidente senior, oficial LSB/ALD/OFAC de Green Dot Corporation y ex asesor senior del Departamento del Tesoro de los EE.UU. en la Oficina de Financiamiento del Terrorismo y Crímenes Financieros. "No importa cómo esté organizado o dónde se encuentre. Importa cómo actúe, los servicios que preste. Si usted es un NSM extranjero que realiza negocios en los Estados Unidos, es un requisito perfectamente razonable que deba cumplir con las regulaciones".

Brinda un mayor acceso a las autoridades de control legal

Cuando se trata de lavado de dinero, Internet es mencionada frecuentemente como el Lejano Oeste. La nueva regla establece un poco más de ley y orden a la frontera cibernética. Si los NSMs extranjeros cumplen con los requisitos, la regla

> La nueva regla establece un poco más de ley y orden a la frontera cibernética

hará que el trabajo de las autoridades de control legal sea un poco más fácil cuando investiguen los delitos transfronterizos a diferencia de aquellos que se cometen el mundo virtual. Al ampliar la definición de aquellos sujetos a las regulaciones LSB y a las obligaciones de conservación de registros y reporte, les brinda a los agentes de control legal de los EE.UU. acceso a la información adicional necesaria para los procedimientos de control legal.

"Si los NSMs internacionales operan de la manera que se supone deben hacerlo bajo la regla, será bueno para las autoridades de control legal", dijo Dennis Lormel, Presidente de DML Associates LLC, y ex jefe del Programa de Crímenes Financieros de la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés). "El tener acceso a la información será una gran ventaja para las investigaciones si estos negocios conservan los registros de la manera en que se supone deben conservarlos".

Si bien la información puede ser una gran ventaja para las autoridades de control legal, las obligaciones de conservación de registros podrían ser un enorme desafío logístico para los NSMs extranjeros. Cumplir con esta obligación es más fácil decirlo que hacerlo, especialmente para las empresas con redes masivas de agentes o aquellos que operan principalmente a través de Internet. La divulgación de la información sobre las obligaciones a los agentes de la primera línea; la capacitación de los empleados, agentes y socios comerciales, y la implementación de sistemas de conservación de registros será una tarea extraordinaria.

"No veo a estas clases de negocios conservando los registros (obligatorios) de la manera en que se supone deben hacerlo", dijo Lormel. "En este punto no tienen la capacidad y entrenamiento para conservar sus registros. Cuando se llega al nivel del agente, no tengo ninguna confianza en su habilidad para conservar los registros. Les va a ser muy difícil a estas compañías porque hay muchos agentes".

Las relaciones bancarias pueden cambiar

Hay menudo existe una relación difícil entre los NSMs y sus bancos. En algunos casos, los bancos inseguros de la base de clientes del NSM, cierran las cuentas existentes del NSM o se niegan a abrir cuentas nuevas. La nueva regla podría exacerbar este problema.

"Podría ser más costoso para el banco para asegurar que los NSMs extranjeros cumplan con las obligaciones de la LSB", dijo Lormel. "Y algunos bancos podrían optar por no hacer negocios con los NSM para no preocuparse de que la cuenta pueda generar temas regulatorios. Con razón o equivocados, podría tener un impacto adverso en los NSMs".

Las preocupaciones por los NSMs podrían ser aliviados si el banco incluyera los nuevos requisitos en su diligencia debida durante la apertura de la cuenta o en su proceso de revisión de cuentas, según Ross.

"Solo se trata de otra pregunta al abrir una cuenta", dijo Ross. "Si el NSM debe inscribirse, entonces debe informar la inscripción. Si el NSM cumple con todos los requisitos, y no existen otros temas con relación a los NSMs extranjeros, entonces no debería haber ningún impedimento para que los NSMs extranjeros puedan abrir o mantener una cuenta bancaria en los EE.UU. Estas nuevas obligaciones no deberían generar obstáculos adicionales".

Mientras el debate continúa en la comunidad ALD, pasarán meses, sino años antes de que puedan evaluarse los efectos finales de la regla sobre los NSMs extranjeros. La regla entrará en vigencia 60 días después de su publicación en el Federal Register los nuevos NSMs alcanzados por la regla están obligados a cumplir con ella dentro de los seis meses posteriores a esa fecha.

Debbie Hitzeroth, CAMS, Oficial de Cumplimiento LSB/OFAC/BIS, Servicio Postal de los Estados Unidos, Washington, D.C., EE.UU., correo electrónico Deborah.L.Hitzeroth@usps.gov

Malasia y el antilavado de dinero

Este artículo contiene un breve panorama de la Ley Anti-lavado de Dinero y Anti-Financiamiento del Terrorismo de 2001 de Malasia (Ley 613), también conocida como AMLATFA por sus siglas en inglés. En particular, se concentra en los últimos agregados a la lista de delitos subyacentes bajo la AMLATFA, refiriéndose a varios delitos relacionados con las declaraciones y pago de impuestos y la operación de esquemas ilegales *Kootu*.

Panorama general de la AMLATFA

La Ley Antilavado de Dinero de Malasia de 2001 (AMLA, por sus siglas en inglés) fue promulgada en enero de 2002. La AMLA ha recibido un nuevo nombre y fue modificada, llamándose ahora Ley Antilavado de Dinero y Antifinanciamiento del Terrorismo de 2001 (Ley 613), la cual entró en vigencia el 6 de marzo de 2007, e incorporaba importantes obligaciones en el área del financiamiento del terrorismo. La AMLATFA penaliza el lavado de dinero y levanta el secreto bancario en las investigaciones criminales vinculadas a 248 delitos subyacentes.

Instituciones reportantes

Todas las instituciones reportantes están sujetas a la misma supervisión de la Unidad de Inteligencia Financiera, la cual a su vez es supervisada por el Banco Central de Malasia y las agencias de control legal. También deben presentar reportes de operaciones sospechosas de acuerdo con la AMLATFA. Entre las instituciones reportantes se incluyen: bancos comerciales, bancos mercantiles, compañías financieras, cambiadores de divisas, casas de descuento, agentes de seguros, operadores de seguros islámicos (Takaful), bancos offshore, aseguradoras offshore, fideicomisos offshore, el Fondo de los Peregrinos (Pilgrims Fund), el Servicio Postal de Malasia, los bancos de desarrollo como el Banco Nacional de Ahorros de Malasia, el Banco de Cooperación Popular y los casinos autorizados. Los controles de lavado de dinero no han sido extendidos a algunas instituciones financieras no bancarias, incluidas las casas de cambio y de corretaje de acciones, o intermediarios como los abogados, contadores y brokers.

Características de un esquema *Kootu*

- Fácil inversión durante un plazo corto de tiempo
- Baja tasa de anticipo de inversión pero bueno retorno
- No hay ventas de productos
- No es necesario un trabajo arduo
- Ganancias obtenidas en base a la contribución de otros participantes
- Ganancia adicional es obtenida cuando un inversor presenta a nuevos participantes
- Adopta modus operandi similar al usado en los esquemas de venta directa

Fuente: Ministerio de Comercio Interno, Cooperativas y Consumo

Últimos cambios a la AMLATFA

Los últimos dos agregados, además de la lista actual de 248 delitos subyacentes, son los siguientes:

1. Delitos relacionados con impuestos

- Omisión de entrega, presentación de declaración impositiva, o de dar aviso del acto sujeto a gravamen a la Junta de Ingresos Internos (*Inland Revenue Board*, o IRB, por sus siglas en inglés)
- Entrega de declaraciones impositivas incorrectas
- Evasión voluntaria

2. Prohibición de llevar a cabo el negocio de promoción de los fondos *Kootu*. La definición oficial de fondos *Kootu* está incluida en la Sección 2 de la Ley 28, Ley de (Prohibición) de fondos *Kootu* de 1971. Ellos son un "esquema o acuerdo a veces conocido como *kootu*, *cheetu*, *chit fund*, *hwei*, *tontina*, o cualquier otro nombre por el cual los participantes suscriben periódicamente a un fondo común y ese fondo común es puesto a la venta o al pago de los participantes en un remate, oferta, licitación o votación. En términos no legales, el fondo *Kootu* puede ser definido en términos generales como un grupo de individuos que acuerda contribuir a un fondo común en intervalos regulares, una suma de dinero acordada previamente en intervalos mensuales o semanales. Los fondos son retirados del fondo común por el individuo a través de un mecanismo de lotería. Por ejemplo, un grupo de 20 individuos acuerda participar en un fondo *Kootu*, y los términos incluyen que cada individuo contribuya una suma fija de RM100 (US$35) por mes durante 20 meses. Utilizando un mecanismo de lotería mensualmente, la persona que es seleccionada primero al azar recibe entonces la suma de RM2.000 en valor equivalente a los 20 meses de contribución de RM100, a pesar de haber contribuido solamente RM100 el primer mes. El sorteo de lotería se realiza mensualmente hasta que los 20 individuos reciben sus RM2.000. La estructura del fondo no tiene como objetivo obtener una ganancia, sino dar un mayor apalancamiento a un grupo pequeño de individuos vinculados financieramente mediante la confianza. Claramente, el fondo *Kootu* beneficia a los individuos que pueden retirarse el fondo al principio del ciclo, y por lo tanto el posible abuso de un esquema de ese tipo es el basarse en la confianza e integridad de los individuos que al inicio del ciclo han recibido sus fondos para que sigan contribuyendo al fondo a fin de que los demás miembros reciban las sumas que les correspondan.

Relación con impuestos

La inclusión de los delitos subyacentes relacionados con impuestos fue promulgada como ley en octubre de 2010. La inclusión de estos delitos subyacentes impositivos ha ampliado los poderes del IRB. Muchos contribuyentes todavía no conocen estos cambios a la lista de delitos subyacentes de la AMLATFA. Ya están siendo investigados unos pocos casos de conformidad con esta nueva sección y se presentarán acusaciones a su debido tiempo.

Es probable que la inclusión de los delitos subyacentes relacionados con impuestos haya sido influenciada por el éxito del Servicio de Rentas Internas de los EE.UU. (IRS, por sus siglas en inglés) en la obtención de aproximadamente 4.550 nombres del UBS AG, donde el banco pagó US$780 millones en concepto de multas y desembolsos.

Fondos *Kootu*

Fue recién alrededor de junio de 2010 que escuché hablar por primera vez de los fondos *Kootu* y posteriormente de la Ley de (Prohibición) de Fondos *Kootu* de 1971. Desde la década del '60 hasta la década del '70, los fondos *kootu* fueron utilizados específicamente por familiares, entre amigos o dentro

de un pueblo pequeño. Muchos encontraron que era muy fácil de usar, como eran los esquemas de micro-financiamientos. El fondo *kootu* o fondo tontina era esencialmente una línea de crédito gratuita basada en la confianza mutua; mantuvo estrechas relaciones e incluso fortaleció las redes entre mujeres profesionales, familiares y amigos. Funciona cuando todos los participantes suscriben periódicamente o de otra forma a un fondo común. Cuando un participante solicita prestado del fondo, cada miembro hará responsable del repago al prestatario. La naturaleza de estos fondos implica que no hay fines de lucro, sino que son un medio para ayudar al prestatario en caso de dificultades financieras o para cualquier otro uso.

Esos fondos aún existen hoy entre los grupos de bajos ingresos y en villas lejanas donde el acceso al financiamiento de las instituciones financieras es casi imposible. El fondo *kootu* podría ser parecido a un esquema tradicional de microfinanciamiento, donde pequeños préstamos de generalmente menos de US$100 son otorgados a la gente pobre de las zonas rurales, especialmente en a nivel de las aldeas.

Como manera informal de solicitar prestadas pequeñas sumas de dinero, los fondos *kootu* son susceptibles de ser abusados. Esto llevó a la promulgación de la Ley de (Prohibición) de Fondos *Kootu* de 1971. Desde entonces, se ha prohibido cualquier esquema de ganancia excesiva de los fondos *kootu* o tontina, y cualquier negocio registrado que dirija cualquier cosa parecida a un fondo *kootu* es responsable y puede sufrir una sanción de hasta RM5.000 y/o una condena a prisión de hasta tres años.

Con tantas otras inversiones reguladas en el mercado actual, ¿por qué la gente invierte en los esquemas *kootu*? ¿Por qué invierten en una inversión de alto riesgo que puede ser objeto de fraude? Un fondo *kootu* o tontina puede generar ganancias de distintas maneras, que van desde la simple selección de grupos hasta subastas entre los miembros. En los casos donde el esquema es tan grande como los de World Heritage Resources, un negocio que fue fundado bajo la Ley de Inscripción de Negocios de 1956 (Ley 197), que tenía más de 300.000 miembros y una suma total de RM30 millones acumulados durante dos años, el riesgo financiero de participar es alto. La alta probabilidad de que los fondos desaparezcan con o sin rastro es muy real, independientemente de si el esquema es operado por un negocio registrado o no. Para agregar un elemento más, los retornos en este caso fueron pagados utilizando giros postales, que no son detectados por el radar de los sistemas sofisticados de lavado de dinero de las instituciones financieras.

El sistema nacional postal, Pos Malaysia Berhad, es una institución que reporta a la UIF del Banco Central Malasia. El Informe de Evaluación Mutua sobre Malasia publicado por el Grupo Asia/Pacífico en julio de 2007 recomendaba que Pos Malaysia "aplique criterios más dinámicos y menos rígidos para detectar sospechas". Sin embargo, los directores de World Heritage Resources se las arreglaron para comprar giros postales por valor de cientos de miles sin generar ninguna sospecha. El informe también indicaba que las presentaciones de ROS por parte de Pos Malaysia habían aumentado diez veces, de 73 en 2005 a 703 en 2006, las presentaciones eran "indicadores de acuerdo con las reglas de los ROSs generados, sin tener en cuenta cualquier sospecha subyacente". Pos Malaysia por ende necesita reducir las falsas alarmas y mejorar mucho la calidad de sus presentaciones de ROS.

Desde 2009 hasta 2010 solamente, han llegado a los tribunales nueve casos por violaciones a la ley. En febrero de 2011, se hicieron modificaciones a la Ley de (Prohibición) de Fondos *Kootu* de 1971 para aumentar las sanciones de RM5.000 a RM500.000 y para incrementar el plazo de la condena a prisión de tres a diez años.

En mayo de 2011, después de los cargos presentados contra los directores y operadores de esquemas *kootu* utilizando giros postales de Kristal Karisma Enterprise, World Heritage Resources y Al Falah Global Resources, negocios que habían sido creados bajo la Ley de Registración de Negocios de 1956 (Ley 197), esos esquemas ilegales han sido incluidos como delitos subyacentes bajo la AMLATFA. Esto les dará a los reguladores la capacidad para congelar dineros obtenidos de manera ilegal proveniente de los esquemas.

A final del día, todavía quedan muchas preguntas con relación a los fondos *kootu* que operan en las aldeas y áreas rurales. ¿Quién va a monitorear a estos fondos operados, ya que no están bajo la supervisión directa del Banco Central de Malasia o la Comisión de Valores? ¿Cuánto puede crecer el fondo sin regulación oficial? ¿Por qué no simplemente convertir todos los fondos *kootu* a una organización financiera similar al Grameen Bank en Bangladesh? Mientras haya dinero involucrado, siempre habrá abusadores, aún cuando los participantes sean respetables, dignos de confianza y solventes. Personajes similares a Bernie Madoff han surgido en los Estados Unidos. ¿Por qué no en Malasia? La inclusión de la operación de los esquemas ilegales *kootu* como delito subyacentes de la AMLATFA simplemente tiene sentido.

Conclusión

Las recientes modificaciones a la AMLATFA son un acto audaz del gobierno malayo y también muestran su seriedad en tratar de combatir las actividades de lavado de dinero.

Aaron Lau, CAMS, CFE, CA (M), FCA (Aust), jefe de investigaciones de fraude y cumplimiento antilavado de dinero, AITLAU Management Services, Kuala Lumpur, Territorio Federal, Malasia,aaron@aitlau.com. Colaboró Hue Dang, CAMS, directora de Asia, ACAMS, hdang@acams.org. Traducido por Yokel Yeung, gerente de desarrollo de asociación, ACAMS,yyeung@acams.org

Capítulo del Sur de California

El Capítulo del Sur de California de ACAMS realizó otro exitoso evento de aprendizaje en junio de 2011 en las oficinas de Wescom Credit Union en Anaheim, California. El tercer evento del capítulo realizado en 2011, que atrajo a más de noventa participantes, fue un análisis profundo del mundo de las investigaciones en Internet. El evento fue una reveladora mirado de las técnicas de investigación más actuales que necesita saber para ser más eficiente en sus investigaciones ALD.

Jane Lee, de Banker's Toolbox presentó el tema realizando una presentación de alto nivel sobre cómo utilizar Internet de una manera más efectiva como una herramienta de inteligencia fuente/competitiva abierta. También reiteró la importancia y aplicabilidad de la investigación efectiva en Internet para la diligencia debida sobre el cliente, el programa de identificación del cliente, y generalmente, el programa de cumplimiento LSB/ALD de la institución financiera.

Michele Stuart, dueña y presidenta de JAG Investigations, Inc., guió a los participantes a través de una cautivante serie de escenarios de investigación destacados y de fuente abierta. Ella presentó a la audiencia técnicas avanzadas para obtener información utilizando distintas herramientas de búsqueda y descubrir información oculta. Continuó su fascinante presentación analizando las estrategias para la filtración, análisis y la organización de información buscada en áreas que incluyen los registros públicos, las fuentes abiertas de Internet, los sitios de redes sociales y la 'Web Invisible'.

La señora Stuart, investigadora privada licenciada desde hace veinte años, ha realizado varias presentaciones a agencias de control legal en los Estados Unidos, en las cuales contó con participantes de Seguridad Interior, U.S. Marshals, FBI, Departamento de Justicia, Naciones Tribales, la Oficina del Fiscal General y varios otros nivel de agencia estatales y federales. Además, como experta reconocida en su campo, ha realizado presentaciones para las industrias financiera y de seguros.

Las presentaciones del evento de Investigaciones en Internet pueden descargarse de la página web del Capítulo del Sur de California de ACAMS http://www.acams.org/communities/chapters/socaln/home/.

El 18 de agosto de 2011 el capítulo organizó el Foro Misto ALD del Sur de California en Irvine, California. Dennis Lormel, consultor senior de DML Associates, LLC, fue el orador principal del evento, el que se realizará a la tarde en la conferencia del Foro ALD de la Costa Oeste. El señor Lormel, agente especial retirado del FBI con 28 años de experiencia, ha acumulado una distinguida carrera, que incluye haber declarado antes numerosos comités del Congresos, la preparación de testimonios para funcionarios senior del FBI y haber actuado como experto en la materia para medios gráficos y de difusión. GlobalVision Systems auspició el evento.

El capítulo concluirá su programa de eventos de 2011 en diciembre con una actualización a ser presentada por la Oficina de Campo de Los Ángeles de la Oficina de Administración de Narcóticos (DEA, por sus siglas en inglés) sobre el impacto de las guerras mexicanas por la droga en el sur de California. Una reunión para celebrar la proximidad de las fiestas concluirá el evento de aprendizaje de diciembre.

En otras noticias, el capítulo le da la bienvenida a Chuck Taylor, del City National Bank como copresidnete, a Susan Wahba de Union Bank como cotesorera, y a Michael Meer del Wilshire State Bank como codirector de comunicaciones.

Capítulo de Australia

Ha sido un invierno muy ocupado para el Capítulo de Australia con varios eventos además de algunos cambios regulatorios importantes tanto en Australia como en Nueva Zelandia. El primer evento del invierno se realizó en mayo. La reunión comenzó con una cálida bienvenida de John Alfano (PayPal Australia) quien amablemente nos ofreció el lugar de reunión y las instalaciones para la presentación. Graham Gorrie (director de programación de Sydney) presentó a Peter Cvetkovski de Risk Associates, quien dio un panorama general del Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI SSC, por sus siglas en inglés) y el proceso de evaluación. Fue una discusión animada, centrada en los 12 prin-

Capítulo Australia continuado

cipales requisitos PCI para la validación. Todas las áreas de cumplimiento incluyen reglas básicas de seguridad que la mayoría de los comerciantes y proveedores de servicios ya deberían aplicar, o estar familiarizados con ellas cuando son auditados. El tema se generó sobre por qué los proveedores de servicios tienen la obligación de cumplir cuando no se trata de una obligación legal, sino que es un estándar requerido por las principales tarjetas de pago (Visa, MasterCard, American Express, Discover y JCB). A fin de combatir el fraude y el lavado de dinero, existe una mayor necesidad de confiar en que los comerciantes procesen los pagos electrónicos en línea y en el ámbito físico. Peter continuó describiendo los distintos objetivos de control relacionados con la dirección de cambio de aplicación (especialmente con relación a la separación de tareas en producción y prueba), los controles de acceso del usuario, la seguridad física y, lo más importante, la documentación. La evaluación pone énfasis en el proceso documentado descripto y en el proceso que efectivamente se aplica. Cuando existe una discrepancia, la organización bajo revisión tratará de entregar documentación para explicar por qué y qué pasos se tomarán para cumplir con los objetivos del control. El salón estuvo concurrido con una animada discusión durante las P&R y el evento culminó con tragos y canapés ofrecidos por by PayPal Australia. Le agradecemos a John Alfano y a PayPal Australia por su amable hospitalidad.

Sydney también fue el lugar de reunión del evento del capítulo organizado en julio. Más de cuarenta miembros del capítulo e invitados estuvieron presentes para escuchar al orador, el Detective John Watson, del Escuadrón de Fraudes, Comando Estatal del Crimen, Policía de NSW, presentar una sesión sobre "Reporte de Tema Sospechoso y el Proceso de Investigación". Después de la presentación se efectuaron varias preguntas sobre los distintos aspectos de la participación de la Policía NSW con el reporte de asuntos sospechosos. La junta desea agradecer a Ernest & Young por la organización del exitoso evento.

El Capítulo de Australia tuvo la suerte de contar con 12 asistentes de Australia que concurrieron a la 3er. Conferencia Anual de Asia-Pacífico de ACAMS, realizada en Beijing el 13 y 14 de junio. Ocho de ellos son miembros del Capítulo de Australia y tres de los ocho son miembros de la junta del capítulo. Fueron presentados una variedad de oradores, incluidos reguladores, oficiales ALD y funcionarios de control legal. Se recibieron varias opiniones fundamentales sobre las tendencias específicas que surgen de la región Asia-Pacífico, incluida la gran preponderancia de familiares vinculados con casos de lavado investigados por la UIF de Taiwán, la amenaza emergente de los proveedores de e-efectivo cuando actúan como clientes de grandes bancos debido a la incapacidad de ver a través de los clientes subyacentes, y varias declaraciones interesantes por parte de la Oficina Antilavado de Dinero, el Banco Popular de China, destacando los enormes recursos y la atención prestada a este tema en el país — resaltándose que en el último año se impusieron más de 250 sanciones contra las instituciones financieras por fallas de control ALD. Los talleres de día completo fueron de un éxito particular, con mucha interacción durante los casos de estudio y los debates sobre qué hace que un programa ALD (y el oficial ALD) sean exitosos, agregando interés a los procedimientos a medida que los presentadores seleccionaron respuestas a escenarios para mostrar que la repuesta obvia del "oficial de cumplimiento siempre era la mejor respuesta para la organización! Como siempre, la habilidad para combinar informalmente con los profesionales ALD fue en sí misma de gran valore, con muchos intercambios de buenas prácticas, novedades de las amenazas emergentes y las tipologías experimentadas por varios delegados. La próxima conferencia APAC de ACAMS se realizará en abril de 2012. Asegúrense de agendar esta fecha en sus calendarios.

Por el lado regulatorio, Nueva Zelandia ahora tiene sus regulaciones ALD/CFT. Hay cuatro conjuntos de Regulaciones que abarcan:

- Definiciones relevantes para las entidades reportantes
- Requisitos y detalles del cumplimiento
- Excepciones disponibles
- Formas de solicitar exenciones ministeriales

Como se esperaba, la fecha de vigencia fue establecida para dentro de dos años — las obligaciones de reporte de las entidades según la Ley comenzarán a regir el *30 de junio de 2013*.

El primer Código de Práctica de Nueva Zelanda está próximo a publicarse. Estará vinculado a temas de verificación de identidad.

Para coincidir con las Regulaciones de Nueva Zelandia, se ha programado un webseminario, el que se realizará el viernes 9 de septiembre.

En Australia, la Ley ALD/CFT ha sido modificada, y se han incorporado normas para considerar el programa de recupero de costos de AUSTRAC además de una regulación más estricta para los proveedores de remesas. La Ley de Sanciones Autónomas de 2011 ha sido promulgada.

La junta nuevamente ha visto cambios en los últimos meses. La junta desea agradecer a aquellos miembros que dejan de integrarla, Bill Brown y Tim Land, por su contribución para ayudar al crecimiento del Capítulo de Australia. La junta tiene el agrado de anunciar que Cassandra Hewitt del ANZ Bank ha aceptado ser miembro de la junta como directora de programación (Melbourne).

Evento del Capítulo Canadiense de ACAMS — Estudios de Casos Canadienses de Lavado de Dinero

Más de 200 profesionales ALD asistieron a la primera sesión de capacitación de día completo del Capítulo Canadiense de ACAMS el 14 de abril de 2011 en el distrito financiero de Toronto. Considero que la sesión fue una excelente oportunidad para aprender más de mis colegas sobre cómo los criminales y terroristas están utilizando los servicios financieros de Canadá para facilitar sus actividades ilícitas. La conferencia estuvo especializada en estudios de casos reales canadienses.

La primera sesión del día incluyó a tres estudios de casos bancarios y se refirió al fraude con anticipo de honorarios, el tráfico humano y el financiamiento del terrorismo.

Capítulo Canadiense continuado

Fue fascinante escuchar acerca de los desafíos de los profesionales ALD al tratar con posibles fondos lavados vinculados directamente a actividades criminales. En un caso, el banco supo que un cliente estaba defraudando a canadienses y decidió que presentar un Reporte de Operación Sospechosa (ROS) — el equivalente canadiense del Reporte de Actividad Sospechosa (RAS) — no era suficiente. El dilema fue que si el banco devolvía los fondos al cliente, podría considerarse que estaba facilitando el lavado de dinero porque el banco tenía razones para creer que los fondos provenían de actividades criminales. En este caso, el banco decidió congelar los fondos y aceptar que podía ser demandado por el cliente. Creo que para las organizaciones más pequeñas, que no tienen los mismos recursos legales que un banco grande, sería difícil congelar los fondos sin fundamentos legales para hacerlo. Creo que habría que decidirlo caso por caso. Pero uno tiene que equilibrar los riesgos legales de congelar los fondos versus una demanda colectiva de víctimas de fraude o la posibilidad de verse involucrado en la facilitación de lavado de dinero.

Otro de los oradores habló apasionadamente sobre cómo podrían los bancos ayudar en la lucha contra los criminales y terroristas. Su exposición también me hizo pensar acerca del desdibujamiento de las líneas entre las empresas privadas y el sector de control legal. Esto es probablemente una buena pregunta para otra sesión pero fue interesante escuchar su presentación.

La siguiente sesión estuvo dedicada a los escenarios de juegos de apuestas. Esta sesión fue entretenida y educativa al mismo tiempo — definitivamente una de las presentaciones más memorables del día. Uno de los puntos fundamentales fue el uso de personal de primera línea para entrevistar a los clientes acerca de sus actividades sin darles información acerca de la posibilidad de presentación de un RAS. Los presentadores dijeron que ellos le entregan libretos al personal de las sucursales para que los usen, incluido el acercamiento a los clientes como si estuvieran haciendo un llamado para hacerles una venta.

Hubo varias otras presentaciones excelentes sobre varios temas durante el resto del día cómo: cómo escribir ROS efectivos; cómo manejarse ante las sanciones; el uso de análisis en la investigación; el nexo entre el fraude y el lavado de dinero, y detección de actividades de hawala. La mejor parte de toda la sesión fue una filmina sobre las lecciones aprendidas del caso de estudio que resumieron sucintamente las lecciones clave que podrían ser utilizadas por los participantes. Una sugerencia para la próxima vez podría ser el tener sesiones de trabajo en las que se distribuiría un caso de estudio y cada grupo tendría que presentar lo que hiciera. Entonces compararía el resultado con lo que hicieron los presentadores y creo que esto generaría una discusión animada.

Además, si bien fue difícil escuchar al director del Centro para la Protección de Niños hablar sobre la comercialización de pornografía infantil, fue alentador ver que el sector financiero está finalmente prestando atención.

Después de escuchar a todas las sesiones, solo puedo desear tener los recursos, herramientas y expertos que tienen los grandes bancos pero entonces no tener que preocuparme por las mismas clases y cantidades de riesgo que tienen. Considero que un cierto nivel de comodidad que tienen estas instituciones financieras grandes, que tienen este nivel de infraestructura que aplican y es muy bueno que deseen compartir sus conocimientos con el resto de nosotros. Creo que es la mayor ventaja de ser parte del capítulo de ACAMS y de participar activamente en los eventos organizados. En general, pasamos un gran día aprendiendo sobre los estudios de casos canadienses ALD y espero ansiosamente más eventos estimulantes del pensamiento como éste. ¡Le hago llegar un gran agradecimiento a la junta ejecutiva del capítulo de ACAMS por reunir otro evento bien organizado y espectacular!

Sal Jadavji, CAMS, CFE, oficial jefe ALD de MCAN Mortgage Corporation

Capítulo de Chicago

Ha sido un año activo para el Capítulo de Chicago de la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS), y el verano de 2011 no fue la excepción. Con una agenda llena de eventos de aprendizaje presentados, el capítulo ha ofrecido una variedad de temas antilavado de dinero (ALD) y oportunidades de contactos sociales con colegas. Los temas de los eventos de aprendizaje incluyeron financiamiento del terrorismo, fraude bancario, y un nuevo foro de "mesa redonda" ALD — una sesión de charla abierta y discusión de ideas. Presentando panelistas expertos provenientes de varias instituciones financieras, agencias gubernamentales y el sector privado, cada sesión es preparada en un esfuerzo por continuar con la misión del capítulo de brindar educación, intercambio de información y oportunidades de contactos con los colegas para los profesionales ALD de toda el área metropolitana de Chicago.

El 26 de mayo de 2011, el Capítulo de Chicago organizó su primer evento de aprendizaje en foro abierto, titulado "Mesa Redonda — Una Oportunidad para Dialogar sobre los Temas Fundamentales de Cumplimiento". La sesión se organizó a fin de destacar los "temas candentes" ALD actuales y a la vez ofrecer una oportunidad a los profesionales ALD del área de Chicago de discutir los temas actuales, inquietudes y preguntas así como también permitir el intercambio de información entre colegas en un foro abierto. La reunión fue auspiciada por Deloitte y se llevó a cabo en las oficinas de la firma ubicadas en el centro de Chicago.

El 10 de junio de 2011, el Capitulo de Chicago organizó un evento de aprendizaje titulado "Financiamiento del Terrorismo — Cómo Combaten los EE.UU. al Terrorismo Rastreando los Bienes", auspi-

Capítulo de Chicago continuado

ciado por el Northern Trust Bank en sus oficinas centrales ubicadas en el centro de Chicago. La reunión fue desarrollada para arrojar nueva luz sobre los aspectos actuales de los esquemas de financiamiento del terrorismo y contó con una presentación realizada nuevamente por los oradores invitados Thomas Moriarty, investigador especial, Oficina del Fiscal Federal, y Patricia Nevin, agente especial del IRS-CI y miembro del Grupo de Trabajo Conjunto sobre Terrorismo. Los participantes recibieron conocimientos de vanguardia del tema presentados por veteranos expertos en el área sobre los medios complejos mediante los cuales las organizaciones y los intereses terroristas internacionales reciben su apoyo financiero.

Finalmente, el 18 de agosto de 2011, el Capítulo de Chicago organizó un evento de aprendizaje auspiciado por Wipfli, LLP, el que contó con el orador invitado Tim Tedrick, Socio, Wipfli LLP. La presentación del señor Tedrick estuvo dedicada a los medios por los cuales las instituciones financieras pueden caer víctimas de esquemas de fraude organizado — tanto interno como externo — y los métodos para ayudar a reducir la probabilidad de futuras pérdidas. Este evento de aprendizaje continúa los esfuerzos de Capítulo de Chicago por destacar la sinergia entre las iniciativas ALD y de fraude y la necesidad de colaboración y eficiencias mejoradas entre los recursos de apoyo de investigaciones dentro de las instituciones financieras. Estos factores entran a jugar especialmente cuando los patrones y tendencias que pueden parecer únicos para cada área requieren una convergencia de investigaciones y la necesidad de intercambio de información.

El Capítulo de Chicago de ACAMS celebrará orgullosamente su tercer aniversario el 11 de septiembre de 2011. Un evento tentativamente programado será una reunión de agradecimiento a los miembros y la presentación de un Nuevo programa de aranceles de membresía del grupo, en fecha a a anunciarse. La junta del Capítulo de Chicago mantiene su invitación a los miembros de ACAMS que nos visiten desde fuera del área de Chicago para que participen en los eventos de aprendizaje para estar en contacto con más colegas.

Para obtener más detalles sobre los eventos anteriores y futuros, por favor visite el sitio web del Capítulo de Chicago en: http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/Chicago/Default.aspx

Evento del Subcapítulo de Edmonton de ACAMS

El Subcapítulo de Edmonton de ACAMS organizó su segundo evento el lunes 30 de mayo de 2011. El Inspector Greg Preston del Servicio de Policía de Edmonton (EPS, por sus siglas en inglés) hizo una presentación sobre lavado de dinero y decomiso de bienes. El Inspector Preston tiene una amplia experiencia el área policial. Actualmente está a cargo de la Rama del Crimen Organizado del EPS. Ha representado a la mayor comunidad policial actuando como asesor legal representando a la Asociación Canadiense de Jefes de Policía ante la Suprema Corte de Canadá en cinco ocasiones diferentes.

El Inspector Preston presentó una perspectiva desde el control legal sobre el lavado de dinero. Analizó varios tipos de grupos del crimen organizado en acción y las actividades criminales que se están viendo localmente y en todo Canadá (p.e., drogas, armas, tráfico humano, telemercadeo, pandillas, fraude hipotecario, cheques falsificados, fraude con tarjetas de débito/crédito, etc.). Además, incluyó las siguientes áreas:

1. Etapas del lavado de dinero, actividades comunes al lavado de dinero, actividades específicas de lavado de dinero (p.e., Casinos, tarjetas prepagadas, cambio de divisas, tarjetas de crédito recargadas, etc.)
2. Lavado de dinero y vacíos en el reporte a FINTRAC (p.e., vehículos, relojes/joyería/obras de arte/fianza y honorarios por servicios legales, etc.)
3. Técnicas emergentes de lavado de dinero como las transferencias por juegos de apuestas en línea y la banca móvil (p.e., transferencias de teléfono celular a teléfono celular)
4. Identificó algunas técnicas antilavado de dinero y otras técnicas que se espera sean convertidas en leyes (p.e., CSC, hacer preguntas, observar la naturaleza de las transacciones, IFs que verifiquen la propiedad que están financiando para confirmar el valor (p.e., viviendas y propiedades agrícolas), dinero en efectivo recibido que sea devuelto (p.e., dinero en efectivo recibido/remitido — reglas para abogados de Ontario, etc.)
5. Pagos de ganancias y hacer que el delito sea oneroso analizando la Ley de Restitución y Compensación de Víctimas e identificando dos áreas: (a) Instrumentos de actividad ilegal (instrumentos del crimen); (b) Adquiridos correctamente mediante un acto ilegal (fondos procedentes de un delito)
6. Decomisos civiles por la Rama del Crimen Organizado EPS de 2010 — identificaba los números y sumas en dólares (p.e., dinero en efectivo, vehículos, joyas, propiedades)

Subcapítulo de Edmonton continuado

Un total de 34 profesionales ALD asistieron al evento. Los participantes provenían del sector de control legal (miembros de la RCMP de Edmonton y Calgary), el Gobierno de Alberta, firmas de servicios profesionales, NSMs, instituciones financieras e investigadores privados.

Los asistentes completaron formularios de evaluación. Las evaluaciones recibidas indicaron que el evento fue un éxito y la mayoría calificó al evento de excelente e informativo.

Estamos planificando la próxima reunión en Edmonton en octubre de 2011.

El Capítulo de Nueva York

El Capítulo de la comunidad de Nueva York de ACAMS asistió entusiasta al evento de aprendizaje de verano titulado "Manejo de una Investigación Gubernamental de Lavado de Dinero de su Institución" realizado el 13 de julio. El programa, organizado por Kroll en The Union League Club, fue moderado por el copresidente del Capítulo Barry Koch y contó con los miembros de la junta Meryl Lutsky y David Chenkin. Asistieron al evento más de 200 participantes.

Lutsky recibió en 2010 el *Premio al Profesional del Año de ACAMS* y ha sido el Director de la unidad de lavado de dinero de la Oficina del Fiscal General del Estado de Nueva York y del Grupo de Trabajo sobre Fondos Derivados de Crímenes del Estado de Nueva York des 2004. Chenkin es socio de la firma de abogados de Manhattan Zeichner Ellman & Krause LLP.

Los dos oradores reseñaron el proceso por el cual las instituciones financieras pueden quedar bajo investigación por parte de las autoridades de control legal. Lutsky expuso la perspectiva del fiscal mientras que Chenkin hizo su presentación desde su experiencia representando a las instituciones financieras.

Lutsky explicó las diversas formas por la cuales su oficina u otras agencias de control legal puede iniciar la investigación de una institución financiera. Mencionó a los empleados que denuncian a las propias empresas *(whistleblowers)*, el escrutinio regulatorio y la información de los ROS presentados como ejemplos de catalizadores. Una manera interesante por la cual los fiscales encuentran deficiencias en los programas antilavado de dinero es a través de la falta de presentaciones de ROSs. Lutsky comentó que si todos los bancos grandes están presentando ROSs regularmente sobre un determinado tema candente (como el fraude hipotecario o con préstamos) y una institución similar no presenta ningún ROSs de este tipo, el silencio explica mucho más que las palabras. La falta de presentación puede hacer que el fiscal tenga dudas sobre los procesos de la institución sobre un determinado producto o servicio.

Chenkin compartió una sigla (en inglés) que se debe aplicar en estas investigaciones. DNILE es la sigla de la frase en inglés *"Do Not Ignore Law Enforcement" (No Ignorar al Control Legal)*. Expuso sobre cómo el estropear una relación con las autoridades de control legal, sea intencionalmente o no, puede perjudicar las posibilidades de la institución de salir indemne de una investigación. Entre los errores comunes se incluye el incumplimiento con los términos específicos de una orden judicial o la demora en la entrega de información. Lutsky confirmó que la cooperación con las autoridades de control legal solo puede ayudar a la institución, y que en el pasado, ha llevado a la indulgencia por parte del fiscal.

Al final del evento realizado en julio, el copresidente del capítulo, Vasilios Chrisos agradeció a Koch por los más de dos años de servicio en la junta del capítulo. El Capítulo de Nueva York se ha beneficiado con una increíble bajo el liderazgo de Koch y Chrisos, habiendo cuadruplicado sus miembros y organizado numerosos eventos de aprendiza y sociales, incluido el evento de aprendizaje de día completo de ACAMS organizado por un capítulo. Koch continuará integrando la junta del Capítulo de Nueva York y será sucedido por la ex directora de comunicaciones Erika Giovanetti.

El Capítulo de Nueva York has planificado una apasionante temporada 2011-2012, incluida la realización de varios tipos nuevos de programación. Para obtener información sobre la membresía o los eventos de aprendizaje recientes, por favor visiten la página web del Capítulo de Nueva York en http://www.acams.org/communities/chapters/nyn/home/. Si desean contactar a la junta directiva, por favor háganlo a acamsnewyorkchapter@gmail.com.

Capítulo del Sur de la Florida

¡El Capítulo del Sur de la Florida de ACAMS organizó un destacado evento de aprendizaje en este segundo trimestre! Continuando con su misión de mejorar el conocimiento, habilidades y experiencia profesional de aquellos dedicados a la detección y prevención del lavado de dinero, el capítulo continuó brindando a sus miembros diversos eventos educativos así también como oportunidades de encuentros sociales con los colegas.

Como saben, en 2009, una orden de la SEC aprobó la Regla del Programa de Cumplimiento ALD de FINRA en 2010, y se emitió una guía conjunta de FinCEN, la SEC y otros reguladores federales sobre la obtención y conservación de la información sobre la propiedad beneficiaria con. Teniendo presente estos acontecimientos, el capítulo organizó un evento especialmente diseñado para broker/agentes, realizado el 12 de mayo, el cual contó con un panel compuesto por miembros prominentes de la industria. El panel estuvo integrado por Peter González, examinador principal y especialista regulatorio ALD de la Oficina del Distrito de la Florida de FINRA. Antes de ingresar a FINRA, trabajó en la Oficina Regional Sudeste de la Comisión de Valores y Bolsas de los EE.UU. (SEC, por sus siglas en inglés). Jeri Dresner es asesora legal especial de la División de Regulación de la Oficina Regional de Miami de la SEC. En este cargo, es asesora legal de las sucursales de Asesores de Inversión, Compañías de Inversión, Broker-Agente, y Agentes de Transferencia, y es el enlace con las autoridades de control legal. Nicholas P Salas es CCO de InterBolsa Securities ubicada en Miami. Con 16 años en la industria, su experiencia anterior incluye haber trabajo, entre otros, en Wachovia Securities, Prudential y Merrill Lynch. A este evento, realizado en el Wells Fargo Bank en Miami y titulado "Modelo de Programa de Cumplimiento ALD para broker/agentes", asistieron numerosos profesionales ALD de distintas industrias. Los expositores fueron entusiastas y destacaron su visión del proceso de debida diligencia, el

Capítulo del Sur de la Florida continuado

proceso de examen realizado por las agencias, las mejores prácticas de cumplimiento y algunos procedimientos recientes de control legal.

La presentación fue dinámica e interactiva durante todo el evento de aprendizaje, con preguntas interesantes por parte de la audiencia. La reunión fue tan amena que se extendió más allá del horario programado. El evento culminó con una sesión de contacto entre colegas seguida de tragos y hors d'oeuvres.

Los miembros de la junta también organizaron el evento social mensual del capítulo el 26 de mayo, en el Fado Irish Pub en el área de Miami-Brickell. Como todos los meses, el objetivo de la reunión fue reunirse con los miembros actuales del capítulo en un ambiente informal, relajado después de la oficina. Fue una gran oportunidad para que todos pudieran analizar los temas importantes para la industria y pasar un buen rato.

La capacidad para realizar investigaciones amplias y específicas y a la vez tener en cuenta a todo el espectro de crímenes financieros es uno de los aspectos más importantes de un buen programa LSB/ALD. El 14 de julio ACAMS organizó un programa de capacitación de día complete para analizar las planificación de las investigaciones en perspectiva con un plan de ejecución, y brindó información detallada y soluciones prácticas a través del uso de casos de estudio, ejercicios prácticos, intercambio de información con colegas y contacto con los pares. La presentación de estos temas la hicieron Dennis Lormel, ex agente especial del FBI quien fue director del Programa de Crímenes Financieros del FBI y Edward Rodríguez, ex director de la División Criminal del IRS. Fue un evento fantástico con gran interacción por parte de los asistentes. La reunión fue seguida de un evento social en el Fado Irish Pub, al que asistió una gran concurrencia.

El capítulo está planificando eventos educativos entretenidos y evento sociales para el tercero trimestre. El Capítulo del Sur de la Florida está comprometido para ayudar a ACAMS en sus esfuerzos globales para trabajar con organizaciones locales para ofrecer a los miembros otros ámbitos para realizar capacitación y exposición en las áreas relacionadas. Para cumplir con este objetivo, el capítulo participará activamente con la Asociación de Examinadores de Fraude Certificados (ACFE, por sus siglas en inglés) y el Instituto de Auditores Internos (IIA, por sus siglas en inglés) en septiembre. La conferencia de un día de duración, abarcará los temas más importantes, incluida la evaluación del riesgo de los Núms., los agentes-brokers y la banca.

Recuerden que la mayoría de los eventos de aprendizaje del capítulo se computan para obtener los créditos de educación constante necesarios para la certificación o recertificación CAMS.

Les damos la bienvenida a todos los miembros de ACAMS en el sur de la Florida para que se unan a nuestro capítulo, e invitamos a aquellos de los sectores público o privado que todavía no se han asociado a ACAMS a que lo hagan.

¡Nos vemos en las próximas reuniones y eventos!

Para obtener más información sobre los próximos eventos o para asociarse al Capítulo del Sur de la Florida, por favor, visite la página web del Capítulo en www.acams.org.

Departamento de Educación y Capacitación

ACAMS Today tuvo la oportunidad de conversar con Altair González, gerente de educación y capacitación de ACAMS.

González ha estado con la Asociación desde hace casi dos años y produce la Conferencia Anual de ACAMS, los Seminarios de Preparación CAMS, la conferencia y serie de seminarios en la región Asia-Pacífico y la Conferencia Caribeña de ACAMS.

Antes de ingresar al equipo de ACAMS, González era gerente de programas de Meeting Dynamics, a una compañía de gerenciamiento global de destino, donde producía eventos de capacitación corporativa en los EE.UU., el Caribe y América Latina. Fuera del ámbito de ACAMS, González dedica su tiempo a realizar actividades de voluntariado en varias entidades sin fines de lucro y es miembro activo de la Liga Junior de Greater Fort Lauderdale.

ACAMS Today: ¿Puedes describirnos un día de trabajo típico?

Altair González: Comienzo mi día leyendo las noticias y artículos relacionados con el ALD/CFT y las alertas de ACAMS para mantenerme informada sobre los últimos temas que afectan a la industria en todo el mundo. El resto del día lo dedico a la producción de los principales proyectos de capacitación y educación de los cuales soy responsable. Esto incluye los Seminarios de Preparación CAMS, la serie de seminarios de Asia y la Conferencia Anual de la Asociación, que se realizará en Las Vegas en septiembre de 2011. Dirigir un proyecto de la magnitud de la Conferencia Anual de ACAMS es una gran responsabilidad. Colaboro muy estrechamente con los equipos de comercialización, ventas y servicio al cliente para asegurar que ACAMS produzca una conferencia con elevados estándares para los miembros.

AT: ¿Cuál considera que es su mayor logro?

AG: Crear la currícula para la 10ma. Conferencia Anual Internacional sobre Antilavado de Dinero de la Asociación ha sido una experiencia extremadamente gratificante. Trabajé estrechamente con John Byrne y el grupo de trabajo de la conferencia — un grupo de veteranos locales e internacionales de la industria — para crear el mejor programa y grupo de oradores en la historia de ACAMS hasta la fecha. Ver crecer a la conferencia en términos de sesiones y asistencia, y ver que se convierte en uno de nuestros mayores eventos es mi logro más importante aquí en la Asociación.

AT: ¿Cuáles son algunas de las metas u objetivos que espera lograr en el futuro dentro de su departamento?

AG: Nuestra meta es continuar dando capacitación relevante que cumpla con las necesidades educativas de nuestros miembros. Nos esforzamos por estar informados y actualizados sobre los desafíos y tendencias actuales en la industria ALD. Utilizamos este conocimiento para crear seminarios en la web y en vivo, talleres y conferencias regionales que ayudarán a nuestros miembros anticiparnos a los esquemas emergentes, estar actualizados acerca de las obligaciones y expectativas regulatorias. Al crear un foro colectivo para que los expertos de la industria compartan sus experiencias y casos de estudio, podemos mantener nuestra programación innovadora y actualizada.

AT: ¿Qué aprendió de trabajar de cerca con los profesionales ALD/CFT en el programa de la conferencia?

AG: He aprendido que la industria ALD/CFT está en constante cambio como resultado de las regulaciones nuevas, los procedimientos de control, las sanciones y los esquemas cada vez más sofisticados que amenazan a las instituciones financieras. Para aquellos que trabajan en el área del cumplimiento, sea que se trate de un agente gubernamental, un NSM, auditor o agente de seguros, el anticiparse a los criminales y sus esfuerzos es la clave para mantener un programa exitoso.

AT: ¿Qué considera que será lo destacado en la conferencia anual de este año?

AG: El año 2011 representa un hito para la conferencia ya que celebramos el décimo año consecutivo de reunir a la comunidad ALD/CFT para intercambiar ideas, estar en contacto con colegas y aprender de los expertos internacionales. Comenzó como una reunión anual de más de 250 miembros y ha crecido hasta albergar ahora a más de 1.000 profesionales ALD de la industria de todo el mundo. La cifra record de oradores reconocidos internacionalmente en la conferencia de este año refleja el enorme incremento en el interés de los profesionales ALD en la capacitación y educación.

AT: Como parte del equipo de educación y capacitación, ¿qué clases de capacitación puede esperar los miembros de ACAMS en 2012?

AG: Para 2012, estamos preparando un programa de capacitación tan diverso como lo son nuestros miembros. Se puede esperar a ver capacitación dirigida no solo a las instituciones financieras sino también a las instituciones gubernamentales y las instituciones no depositarias. Ampliar nuestras ofertas educativas a toda la industria afectada por el lavado de dinero es una meta fundamental de la Asociación. De la misma manera que los criminales descubren actividades ilícitas nuevas, los profesionales ALD de todo el espectro financiero deben estar equipados y preparados con las herramientas y estrategias adecuadas para combatir a esos delitos.

Happy 10th Anniversary ACAMS

SightSpan, Inc.®
Dubai, UAE
Office Building 3,
Green Community
Ground Floor
Dubai Investment Park
Phone: +971 (0)4 801 9254
Fax: +971 (0)4 801 9101

SightSpan, Inc.®
Corporate Headquarters
301 South Broad Street
Mooresville, NC 28115
Phone: +1 704 663 0074
Fax: +1 704 664 2807

SightSpan, Inc.®
New York
5 Penn Plaza, 19th Floor
New York, NY 10001
Phone: +1 212-849-6841
Fax: +1 212-849-6901

SightSpan, Inc.®
Singapore
UOB Plaza 1, 80
Raffles Place
Singapore, 048624
Phone: +65 (6)248 4688
Fax: +65 (6)248 4531

www.sightspan.com