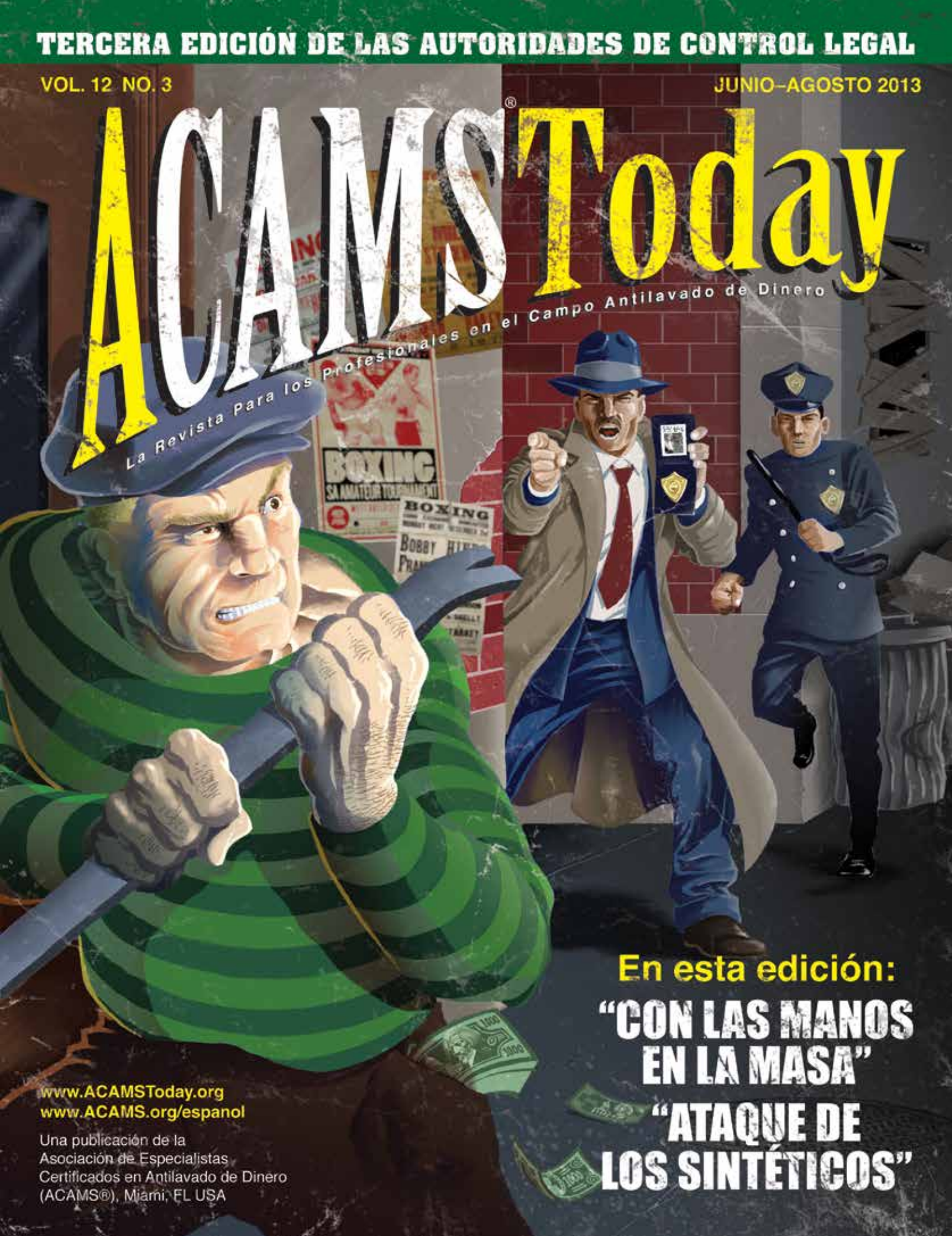
TERCERA EDICIÓN DE LAS AUTORIDADES DE CONTROL LEGAL

VOL. 12 NO. 3 JUNIO–AGOSTO 2013

ACAMS® Today

La Revista Para los Profesionales en el Campo Antilavado de Dinero



En esta edición:

"CON LAS MANOS EN LA MASA"

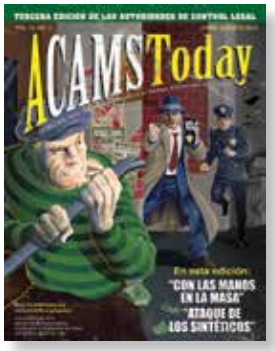
"ATAQUE DE LOS SINTÉTICOS"

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

Una publicación de la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS®), Miami, FL USA

ACAMS® | Advancing Financial Crime Professionals Worldwide®

EN LA PORTADA



Con las manos en la masa

38

Ilustración por Jason Robinson

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

ACAMS® TODAY

EN ESTA EDICIÓN

Uno de mis pasatiempos es hacer compras (sé que muchos de ustedes estarán pensando — por supuesto — eres mujer); sin embargo, no a todas las mujeres les gusta comprar en el sentido de ir a un centro comercial, pelearse con las masas y ponerse a buscar descuentos. En realidad, la experiencia de hacer compras ha cambiado en el último decenio. Muchas de mis amistades hacen sus compras en línea y nunca ni una sola vez entran a una tienda de ladrillos y cemento. Todo esto me hizo considerar lo vigilantes que tendríamos que estar en relación a los delincuentes que se dedican al delito financiero que están al acecho en cada esquina o, debería decir cada navegador, para robar nuestras identidades o para estafar.

El artículo principal *Con las manos en la masa* (página 38) nos enseña la importancia de estar preparados y de cómo estar siempre un paso por delante del delincuente. Los delincuentes se encuentran motivados, y si queremos ganar la batalla contra el delito financiero tenemos que estar más preparados que nuestros adversarios.

El segundo artículo *El ataque de los sintéticos* (página 24) explora una nueva manera que tienen los delincuentes para obtener ventaja sin siquiera necesitar a una persona real, en vez, han tomado el camino menos transitado y creado una identidad sintética. Como profesionales de la prevención del delito financiero, ¿qué podemos hacer para obstaculizar las identidades sintéticas cuando tratan de explotar las instituciones financieras? Aprenda usted los pasos que tendría que tomar y lo que tendría que buscar cuando se enfrenta a un posible ataque de identidad sintética.

Esta edición especial de *ACAMS Today* también contiene tres entrevistas de lectura obligatoria con mujeres tanto del sector público como del privado: Karen O'Brien, la dueña de Global Compliance Solutions; Deborah Morisey, agente especial asistente encargada de las Investigaciones de Seguridad Nacional en Miami; y Lisa Grigg, directora de Fraud Investigations Group en la División de Cumplimiento de Delitos Financieros globales en el Bank of America Merrill Lynch.

En el artículo *¿Cuál es el valor de su evaluación de riesgo?* Los autores definen la importancia de las evaluaciones de riesgo y de cómo una evaluación de riesgo adecuada puede ayudar a la comunidad de aplicación de la ley a detectar, investigar y enjuiciar efectivamente la actividad delictiva.

El monte de tres barajas en el ALD comenta los pasos que usted puede tomar para convertirse en un investigador centrado y no confundirse con el juego de manos del delito financiero. En algunos juegos es mejor ser un espectador y no un jugador.

La sección *Aspectos de Asia* detalla un caso interesante en el que la vigilancia de un cajero ayudó a los representantes de la ley y a la institución financiera a conducir una investigación fuerte en contra de un esquema Ponzi elaborado llevado a cabo por Dream Company. Aprenda las técnicas investigativas aplicadas en este caso y lo que llevó al descubrimiento del esquema Ponzi.

También, el momento de votar los premios de ACAMS ha empezado. Asegúrese de enviar su propuesta de artículo favorito de *ACAMS Today* de 2012 a editor@acams.org al 31 de julio a más tardar. Se anunciará al ganador en la *12 Conferencia Anual de ALD y Delito Financiero de ACAMS* en Las Vegas, Nevada. Para más información sobre los premios ACAMS visite acamsglobal.org.

Los pondrá contentos saber que mientras escribía este artículo compré (sí, en línea) una hermosa billetera rosa que promete proteger mi identidad incorporando una tecnología de protección que lo escuda a uno bloqueando las ondas de radio de los posibles delincuentes que desean robar la información valiosa que pueda haber en la billetera. Esperemos que cumpla con lo prometido.

Karla Monterrosa-Yancey, CAMS
jefa de redacción

Febrero–Abril Graduados CAMS

Andreas Aaris-Larsen
Mohammed Abdul Mateen
Mohammed Abdullah
Kevin A. Aberg
Samer H. Abu Sammour
Julio Acevedo
Sridhar Adepu
Binod Adhikari
Rishi Agrawal
Daniel Aguirre
Naima Ahmad
Haseeb Ahmed
Jabril Ahmed
Hani Al Hares
Hussein M. Al Jaafreh
Amer Al Juqqa
Ihab Ishaq Al Mounyer
Riham Ahmad Al Mousa
Mirna Al Sayegh
Mohammad Farhan Al Swaiti
Saleh Al-Anezi
Erwin Albines
Jaber Mohammed Al-Harbishi
Jamal Abed AL-Kadash
Ismaeel Almeer
Ghaith Al-Nabulsi
Mohammad Bashar Al-Sarraj
Thamer Bassam Alzaidat
Ivan Amaya Gutiérrez
Kay E. Ambrose
Shyamendren Anandakrishna
Frederick Anarfi
Mark Anderson
Jayakumar Annalath
Motasem Arafat
Dmitry Aristarkhov
Amy Arker
Suzanne Arnold
Sylvana Nadim Assaad
Patricia Aurand
Hakeem Damola Ayantayo
Stephan Badenhorst
Muayad Mahmood Bahram
Amy Baird
Charles Baker
Harikrishnan Balakrishnan
Martyna Banaityte
Peter Charles Barnes
Donnalisa Baron
Robert Bassett
Aleksandra Bates
Michelle Bauman
Nancy Baunis
Leslie Bayless
Christina Beadle
Joseph E. Belek
Geneva Belteton
Sara Bennington
Szilvia Bercsenyi
Arjen Michiel Remco Berghouwer
Steven Berry
Jochen Best
Jonathan Betanoff
Rajnish Bhardwaj
Amit Bhatia
Hua Bin
Mary L. Birkentall

Latisha M. Bjone
Remco Boer
Mary K. Bolte
Karen Borgesi
Maria Luisa Boyd
William Yamike Brew
Kairiin (Karen) Bright
Marjorie Britton
Alston Brown
William Brian Browning
Horst Brunner
Jonathan H. Burke
Margaret Burlew
Ryan A. Buxton
Kenneth Call
Sean Cameron
Marci Canaca
Silvia Casariego
Jesus Casillas
Mara Ceason
Denise Cespites
Jung Hyun Cha
Gavin Chamberlain
Angus Champion De Crespigny
Benny Chan
Linda Chan
Piyush Chandra
Jose R. Chavez
Huiming Chen
Jie Chen
Kien Pin Chen
Qianbo Chen
Alex Kin Ming Cheung
Lai Yee Alice Cheung
Kyla Chevett
Christine Seok Chin Loo
Tiffany Chiu
Lionel Chogugudza
Cheng Chong
Wilson Chow
Sarah A. Christian
Mylah Chu
Ian Cilia
Jessica Clarance
David Coleman
Robert N. Collier
Pamela Connell
Chad Cosgrove
Cheryl D. Cote
Sean Crabson
Lewis James Crane
Juan Csillagi
Eniko Csiszer
Chengxia Cui
Zhizhong Dai
Joan Dal Bianco
Majed Dalloul
Namrata Dang
Neibert David
Paul Davidson
Chi T. Davis
Melbith Davis
Solomon Dawson
Odessa L. Dayondon
Maria De Agustin
Chandima De Silva
Kristie Dean

Adam W. Delderfield
David R. DeLeon
Michele Dennis
Ryan Denon
Luis Esteban Depetris
Stamatina Diamantara
Katie Diener
Bruno DiGioacchino
Qin Dong
Rongguo Dong
William A. Douglas
Scott B. Downing
Michael Dressen
Joanna Du
Karen Dussault
Sandeep Dwarakanath
Alex Eadie
Jorge Echarte
Stephen Ediale
Frederick Ehlers
Munaza Ejaz
Salaheddine El Gbouri
Cy Elliott
Elsadiq Osman Abd Elmagid Hamed
Chad Engbrecht
Golnaz Ensan
Theresa Ermer
Alfred Escamilla
Pansiree Euaraksakul
Steffen Exner
Bin Fang
Joyce Lung Fang Hsu
Emily Nadim Fares
Michelle Faulknor
Edward Feistl
Tian Feng
Juan E. Fernandez
Tiffany Fisher
Chad Fishter
Georgina Fitzpatrick
Karla Flores
Jonathan Forth
Sherry Francella
John G. Francis
María Betsabe Franco Maradiag
Mijail Friedman
Ross Fujii
Anthony Gagliano
Sivakumar Ganapathy
Ming Gao
Nandi Gao
Yang Gao
Jose Angel Garcia
Kristi Gary
Julie Gauthier
Ghada Rachid Gemayel
Alexander Gessen
Kara Gifford
Brandon Gilchrist
Sherryl Gilfillian
Andrew Francis Gilmore
Jeremy Glicksman
Mateusz Glowiak
Dmitriy Goldvekht
Francis Gonzalez Mendez
Debra M. Gowins
Andrea Grande

Anthony Green
Aaron Griedl
David John Griffith
Richard M. Grossman
Martin Hacek
Michael Hackenburg
David Haghighi
Dean Hahn
Vahe Hakobyan
Kelly M. Haller
Ramzi Bou Hamdan
Zaid Hameed
Edwin Hammett
Priyanka Sudhir Hampras
Patricia Harris
Shanai Harris
Nick Hartofilis
Mudassar Hassan
Ryan Hatch
Barbara I. Hawkins
Yanli He
Maureen Hellstrom
Courtney Henderson
Lauren F. Henry
Casey Herning
Damian M. Himpsl
Chun Ho
Brian Hollas
Troy L. Hopper
Oliver Housden
Fei Huang
Kejie Huang
Wei Huang
Xiaoqin Huang
Amber Huck
Charles A. Imwalle
Carlos Isarraras
Nawal Itani Al Khatib
Charles Jackson
John J.A. Jacobs
Neha Jain
Haidar Jamal
Nigel James
Suraj Jani
James Jefferson
Andre Jeremiah
Adrianne L. Jerry-Poitier
Wen Jiang
Brian C. Jobe
Alicia Marie Johnson
Mark Johnson Schimmel
Michael A. Jones
Ng Ka Tai
Priyanka Kadam
Joseph Kaltz
Ryoko Kamae
David Karp
Christopher Keller
Evan Kelley
Ryan Kellogg
Roula Maurice Kesrouani
Sabrina Khan
Ronald Kimbrough
Joshua R. King
Ashley Aushra Kirimdar
Jeroen Van Der Klaauw
David Knoedler

Joseph K. Kochuba
Mazahir Kothari
Jiazheng Kou
Philippe Kouassi
Dennis Kroontje
Brian Kruher
Fergal Fong Lai Kuk
Mandeep Kumar
Keeley Kuperus
Oksana Kyrychenko
Steven LaBarbera
Philip S. Lafresnaye
Cathy LaFurge
Alysha Lakdawalla
Linda K. Lakin
Glenn Lambe
Roland Langer
Patricia Lantzy
Myrugia Larmonie
Melissa Larson
Alberto Laureano
Candy Yuen Yan Law
Rossetti Law
Yuliang Le
Sibylle Leboutte
Chi Ying (Elva Claire) Lee
Jennifer Lee
Miriam Lee
Sau Lee
Laureen Lehnberg
Astrid Leigh
Daniela Leon
Jos Leppers
Annie Leung
Debbie Lewis
Guang Li
Haixia Li
Yip Ki Li
Stephanie Liantonio
Edmund Yiok Leng Lim
Tony Lim
Jie Lin
Sheng F. Lin
Michael Little
Chen Liu
Hongwei Liu
Jie Liu
Shu Liu
Yanbin Liu
Matthew Livesay
Brett Logan
Julia Lordi
Krista Loucks
Courtney A. D. Louvar
Miranda Renay Love
Jiangang Lu
Jingjing Lu
Xingzhong Lu
Jennie Lum Laffo
Bangning Ma
Itria Yat Hung Ma
Zhi Ma
K. Karlos Mackey
Inass Madani
Omar Magana
Shweta Mahajan
Brendon Maloney

Melanie N. Manix
Maria Mannone
Emilia Manoilova
Nadeem Hatem Mansour
Archiebald Marchan
Michael Margelewski
Maria Juliana Marra
Lynn A. Martin
Autumn Martinez
Fernando Martins
Nabil Mahmoud Masri
David May
Katherine May
Brian Mayfield
Andrew P. McCarthy
Brad McGovern
Ryan McHale
Nastaran Mehr
Trevor Mendez
Mayra Menendez
Fei Meng
Nicholas Menzorio
Edyta Mieczkowska-Letke
Jason Miller
Jennifer Miller
Lee K. Miller
Joe Millner
Manelik Jose Minaya
Amanda C. Miralrio
Holly Mitchell
Seth Mitchell
Darwin Mitra
Ajaya Mohanty
Erin Mohney
Craig Scott Money
Anthony Morelli
Maya A. Mroue
Lina Ahmed Muheisen
Valerie L. Mulhall
Theresa Munro
Vidya Murali
Jennifer L. Musante
Walid Ismail Mutaw'e Al-Tamimi
John Muvavarirwa
Firas Naber
Yuusuke Nakamura
Anand Narayanan
Divya Narula
Shereen Nasr
Umar Nawab
Godlove Ndangeh
Cory Nealy
Sami Wafic Nehme
Cheri Nelson
Sarah Neri
Katherine Ng
Margaret Tien Che Ng
Terry R. Nickel
Craig Niswander
Yunqing Niu
Geneva Nixon
Simon Norton
Patricia Núñez
Kyle Oakland
Brian Oaxaca
Jason Oberhausen
Joseph Odeyemi

Shanna Ogundiran
Abimbola K. Ogunleye
Chukwunonso Okoro
Lisa Oneil
Hwee ling Ong
Jordan O'Regan
Diana Ortiz
Paul Osborne
Preston J. O'Toole
Robert A. Oven
Karoll V. Palacios
Rui Pan
Dipankar Panda
Ginette Parkin
Richard Perez
Clint Pergram
Diana Perlman
Dianand Persaud
Todd Peterson
Kathlyn Petrillo
Patrick Pfeil
Deepa Philip
Stephen Phillips
Sidris Phipps
Jennifer Pici
Katie Polhamus
Malsie Pomares-Ebanks
Ian Ponman
Anissa N. Powell
Annie Maria Powell
Muhammad Shafi Poyilan
Anitha Pradeep
Elka Karene Price
Doug Princell
Chunhua Qin
Ataur Rahman
Beverley Rahming
Wulfran Ramos Sarmiento
Nicole Rankin
Rajan Rao
Brandon Reddington

Jarvis D. Reeves
Jacqueline Reyes
Brian Rice
Dahlia Rivers
Greg S. Rizzo
Katharine D. Robertson
Kelvin Demetric Robinson
Isaac Rodriguez
Sean Rodriguez
Clare Rogers
Stephen Rogerson
Jeremy C. Rohn
Francisco Gabriel Romo Navarrete
Janet Rose
Daniel Rosenberg
Amanda Rossi
Catherine Roth
David Rowley
Francis Rozario
Jason L. Rumburg
Caitlin E. Ryan
Robert Ryan
Nadezhda Ryzhova
Michael Sacks
John Sagness
Kalpesh Suresh Salunke
Sailaja P.R. Salveraj
Dorra Sanford
Shanti Haslim Sariputra
Zoe Lo Sau Ha
Leslie Sauer
Maria S. Savova
Simon A. Schneider
Natalie Schoon
Matthew Scoll
Michael Scopelliti
Divya Seth
Kim Shackelford
Tapan Shah
Anas Asem Shahin
Muhammad Shakil

Cindy Shao
Geetu Sharma
Bennie Shen
Pei-Yi Shen
Xiaomin Shen
Catherine Shepardson
Yi Fu Shiao
Vincent Shum
Luana Simpkins
Moti Lal Singh
Shashi K. Singh
Anthony Siska
Pavan Sivram
Kimberly K. Slone
Chevaughn T.O. Smith
Sara Joann Smith
Claire Smollett
Greg Solomon
James Song
Yu Song
Benoit St. Georges
Adrian St. Vaughan
Casey Stein
Ken Stoner
Mark Straaten
Diana Strade
John Stribos
Liang Sun
Wenheng Sun
James D. Sutton
Shinichi Suzuki
Harry Swain
Shawna Sykes
Avnish Tahim
Zhiqiong Tang
Trevor Tansey
Shayne Tenpow
Ajeya Thakur
Anuja Thakur
Marsha A. Thomas
Catherine Thompson

Tonia M. Thompson
Wayne A. Thompson
Daniel Thorn
Chi Lai Ting
Nipha Tinto
Henrik Toivonen
Ji Ying Tok
Andrew Tourney
Ramesh Tr
Donna Trapp
Stephanie D. Trotman
Andrea Trujillo Al-Attar
John Tsaboucos
Wing Tsang
Kimberly Tufte
David Tulbert
Steve Twilton
Patricio Bolivar Urquizo Andrade
Robert J. Van Den Berg
Gerasimos Vasilatos, Sr.
Vasanthakumar Venougobal
Javier Vera
Gustavo Vianna-Biehler
Monique R. Victor
Danielle A. Vinje
Joseph Voiro
Brandy Wagner
Cindy See Wai Chew
Chan (Vivien) Wai Yan
Roger Waiters
Joshua Walker
Wendy Wan
Arami Wang
Ying Wang
Ian Wanga
Teresa Waterbury
Susan Watson
Paul Webre
Yangyang Wen
Steven Wickens
Leigh A. Willis

Jonathan O. Wise
Colin Wood
Sharon Worsley Dean
Xiaoyun Wu
Yan Wu
Ying Wu
Zhiyong Wu
Todd Wyer
Jubin Xavier
Min Xie
Xiaojuan Xun
Negin Yahyaei
Huichi Yan
Desiree Yang
Guanghong Yang
Ling Yang
Mingfen Yang
Zhihua Yang
Amanda Yarber
Yu Ye
Minakshi Yerra
Kelly Yeun
Chenyue Yin
Vera Yu
Minmin Yuan
Saleh Waleed Zaki
Dong Zhang
Jinqiang Zhang
Liang Zhang
Weihong Zhang
Zehua Zhang
Meng Zhao
Na Zhao
Maria (Hai Yan) Zhu
Birong Zhuang
Xun Zhuang
Yong Zou
Craig Zwarych

Robert Hawkes
Whitby, ON, Canadá

La carrera de Robert Hawkes abarca 23 años en la policía. Es miembro del Servicio de Policía Regional de Durham, Unidad de Inteligencia — Confiscación de Activos y el jefe de equipo para la Unidad Provincial de Confiscación de Activos.

En los últimos ocho años se le ha asignado a investigaciones de Ingresos Delictivos/Confiscación de Activos donde ha sido el investigador principal en una serie de investigaciones de Delitos de Grupos Organizados tales como Hells Angels, los Banditos y grupos delictivos de Europa Oriental. En esta capacidad ha utilizado con éxito los estatutos Federales, Provinciales y Civiles para incautar y confiscar un sitio de reunión, Hells Angels Clubhouse, y la residencia de un líder del grupo Bandito Outlaw Motorcycle.

Además, Hawkes ha estado involucrado en incautar más de $10, 000,000.00 en ingresos delictivos y la confiscación de más de $3, 500,000.00 en los últimos cinco años.

A Hawkes se le reconoce como un experto en los temas de lavado de dinero, ingresos debidos al delito, contrabando de dinero en efectivo, mensajerías de dinero y propiedad relacionada con el delito. También es instructor en el Toronto Police College, el Canadian Police College, el Ontario Police College y para el Servicio de Inteligencia Delictiva de Ontario (CISO por sus siglas en inglés).

Hawkes también ha capacitado en el Simposio Anual de Lavado de Dinero, el Foro de Ontario sobre Crimen Organizado y en la Conferencia de Capacitación de Lavado de Dinero en Canadá.

Orasa Shirley Patterson, CAMS
Tampa, Florida

Orasa Shirley Patterson es una analista superior de cumplimiento de ALD en Citigroup en Tampa, Florida. Patterson coopera con la Revista de Transacción Periódica (PTR por sus siglas en inglés) analizando transacciones y patrones de transacciones relacionados con la actividad de clientes de Bancos Extranjeros Correspondientes. Patterson asiste en mejorar los robustos procesos de KYC, asegurando el cumplimiento por parte de Citi con expectativas y requisitos regulatorios.

Antes de trabajar en Citigroup, Patterson tuvo exito en la industria de seguros en tanto especialista en servicios de aseguradoras de autos con State Farm Insurance en DuPont,Washington. Aparte de registrar información sobre los clientes, Patterson investigaba sobre y aclaraba discrepancias para los clientes, permitiendo el procesamiento de las políticas de seguros. En su trabajo, Patterson creó y procesó una variedad de informes para asegurar el cumplimiento de las leyes estatales y federales.

Patterson también trabajó como agente de llamadas en EnBW Energie Baden-Wuerttemberg AG Karlsruhe, la tercera empresa en tamaño de utilidades en Alemania. Contribuyó a mejorar la satisfacción del cliente ocupándose de y remediando barreras contractuales al inicio de la liberalización del mercado energético en Alemania.

Patterson tiene un título de BS (Magna Cum Laude) en contabilidad y administración de negocios. Está cursando la MS en Gestión de Seguridad Nacional. Patterson habla tailandés y tiene fluidez en inglés y alemán. Es socia activa de ACAMS.

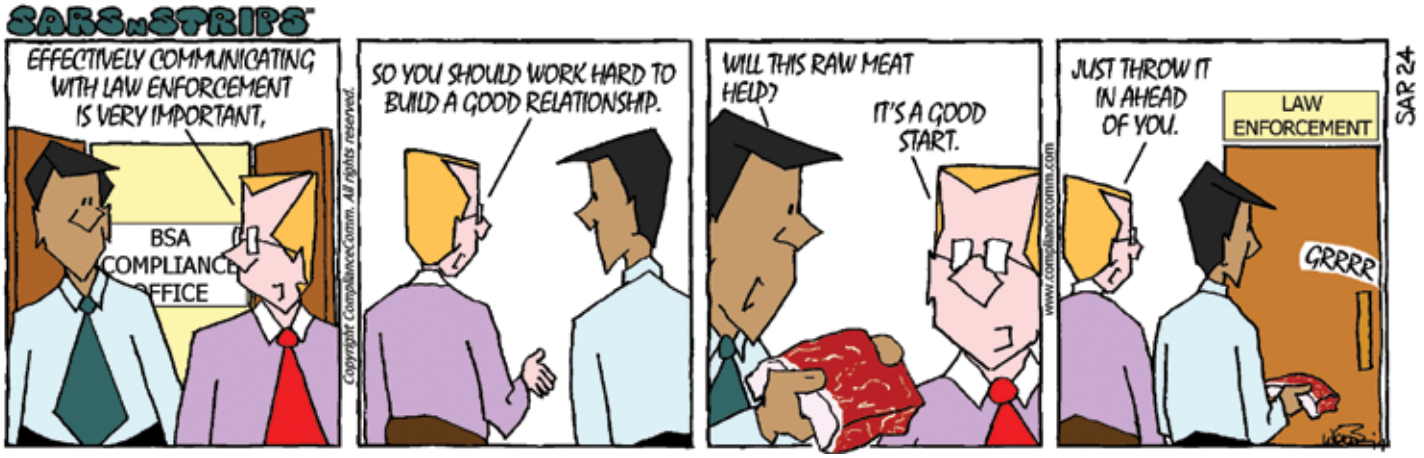
Tom Totton
Muscat, Oman

Thomas Totton es un profesional superior de banco con más de 30 años de experiencia en una variedad de cargos en numerosas empresas de servicios financieros.

Es un banquero calificado, Socio del Instituto de Contadores Públicos en Irlanda y está graduado de la Universidad de Ulster. Recientemente, Totton recibió el Certificado de Honor W. S. Smith de parte de Global IIA por desempeño sobresaliente en los exámenes de la CIA. Aprobó el Examen de Fraude Certificado y obtuvo una evaluación (con mención de distinguido) de parte de la Asociación Internacional de Cumplimiento. Además, completó el Diploma CIMA en Finanza Islámica, obtuvo su Certificación en Seguro de Gestión de Riesgo (CRMA en inglés), un Certificado en Gestión de Seguridad de Información (CISM en inglés) y se presentará a los exámenes de CAMS en 2013.

Totton tiene mucha experiencia en filiales bancarias, finanzas, arriendos, tesorería, consultoría internacional y en auditoría interna. Ha trabajado en diferentes niveles en el Grupo AIB, ha tenido papeles de funcionario superior en el Bank of Scotland (Ireland) Ltd y actualmente es el gerente general/auditor interno en jefe del Banco de Muscat.

Además, Totton es vicepresidente del Capítulo de Omán de IIA y participa de manera habitual y hace presentaciones en los eventos de IIA.



Producido por ComplianceComm

Colaboración y certificación avanzada

Han pasado muchas cosas desde la edición del año pasado de *ACAMS Today*, "De Las Autoridades De Control Legal".

Hemos mejorado el acceso que tienen ustedes a los líderes clave de la comunidad del antilavado de dinero por medio de entrevistas expandidas en nuestra versión en línea de *ACAMS Today*. Además, la aplicación móvil elimina cualquier excusa para no acceder fácilmente a estos mismos artículos y entrevistas, y hasta hemos añadido unos cuantos "podcasts" que planeamos ampliar en 2013-14. Con todos estos canales de reparto, ACAMS continuará necesitando los conocimientos, sugerencias y orientación de ustedes sobre temas, autores, entrevistados y dirección general para ayudar a los socios en nuestro objetivo común de aumentar nuestro conocimiento colectivo y nuestra experiencia.

Nuevas y emocionantes asociaciones para ayudar a la comunidad de prevención del delito financiero

Otro desarrollo en lo cual ACAMS asistirá a los que necesiten pericia investigativa financiera es la asociación entre ACAMS y Utica College. Utica College es la primera universidad del país en establecer un programa de grado en la investigación de delitos económicos y una Maestría en la gestión de delitos económicos.

La asociación extenderá beneficios muy importantes a los alumnos virtuales y del campus de Utica College, incluyendo la membresía gratuita para estudiantes hasta por dos años, como también la oportunidad de tomar el examen de certificación de CAMS al graduarse. Los socios actuales de ACAMS también se beneficiarán de un descuento en la mensualidad y se les dispensará de abonar la cuota al solicitar entrar a los programas en línea de Utica College.

En la escala internacional, Charles Sturt University en Australia se ha asociado con ACAMS para proveerles a los estudiantes de postgrado la orientación necesaria con materiales para que cada alumno pueda completar con éxito el examen de evaluación y acreditación para lograr ser un Especialista de Antilavado de Dinero Certificado (CAMS) como parte del curso. Como ha dicho la Universidad, "Esto quiere decir que los alumnos se graduarán con un diploma doble, el título de CSU y la evaluación de CAMS, así aumentarán notablemente sus conocimientos, capacidad pericial, y posibilidad de emplearse en este sector creciente".

A ACAMS le encanta ser parte de este nuevo ofrecimiento ya que no hay un programa similar de Maestría en ninguna universidad internacional. Por consiguiente, estudiantes de postgrado de Australia, los Estados Unidos, Nueva Zelandia, Canadá, Tanzania, Singapur, Suiza e India ya se han matriculado en este programa, y el curso le servirá a oficiales de prevención/cumplimiento de AML/CTF, a la industria financiera, bancaria, de aplicación de la ley, agencias regulatorias y a otras industrias relacionadas en los Estados Unidos e internacionalmente.

Estamos convencidos de que estas dos asociaciones mejorarán grandemente las relaciones de ALD del sector público y privado que exigen informes efectivos, destrezas investigativas profundas y políticas sólidas de ALD.

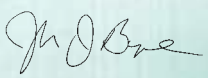
Certificación Avanzada — la próxima herramienta para el éxito de la prevención del delito financiero de AML/CFT

Cuando publicamos la Edición de Las Autoridades De Control Legal de *ACAMS Today* 2012, justo habíamos empezado a desarrollar la certificación avanzada de ACAMS. Bueno, las clases inaugurales de "CAMS-Audit" tuvieron un gran éxito, debido al Comité de Conducción de la Certificación Avanzada formado por profesores expertos y debido al excelente estudiantado. Las clases fueron extremadamente interactivas y el intercambio de información fue de doble vía — tanto hacia los alumnos como hacia los profesores. La próxima parte del proceso de CAMS-Audit consistirá en las investigaciones que deben entregar los alumnos para fin de 2013 y que se compartirán en una biblioteca para los socios de ACAMS. Ahora, tomaremos el mismo formato de certificación avanzada y crearemos el próximo nivel avanzando su educación de CAMS con CAMS-FCI o Investigaciones de Delitos Financieros.

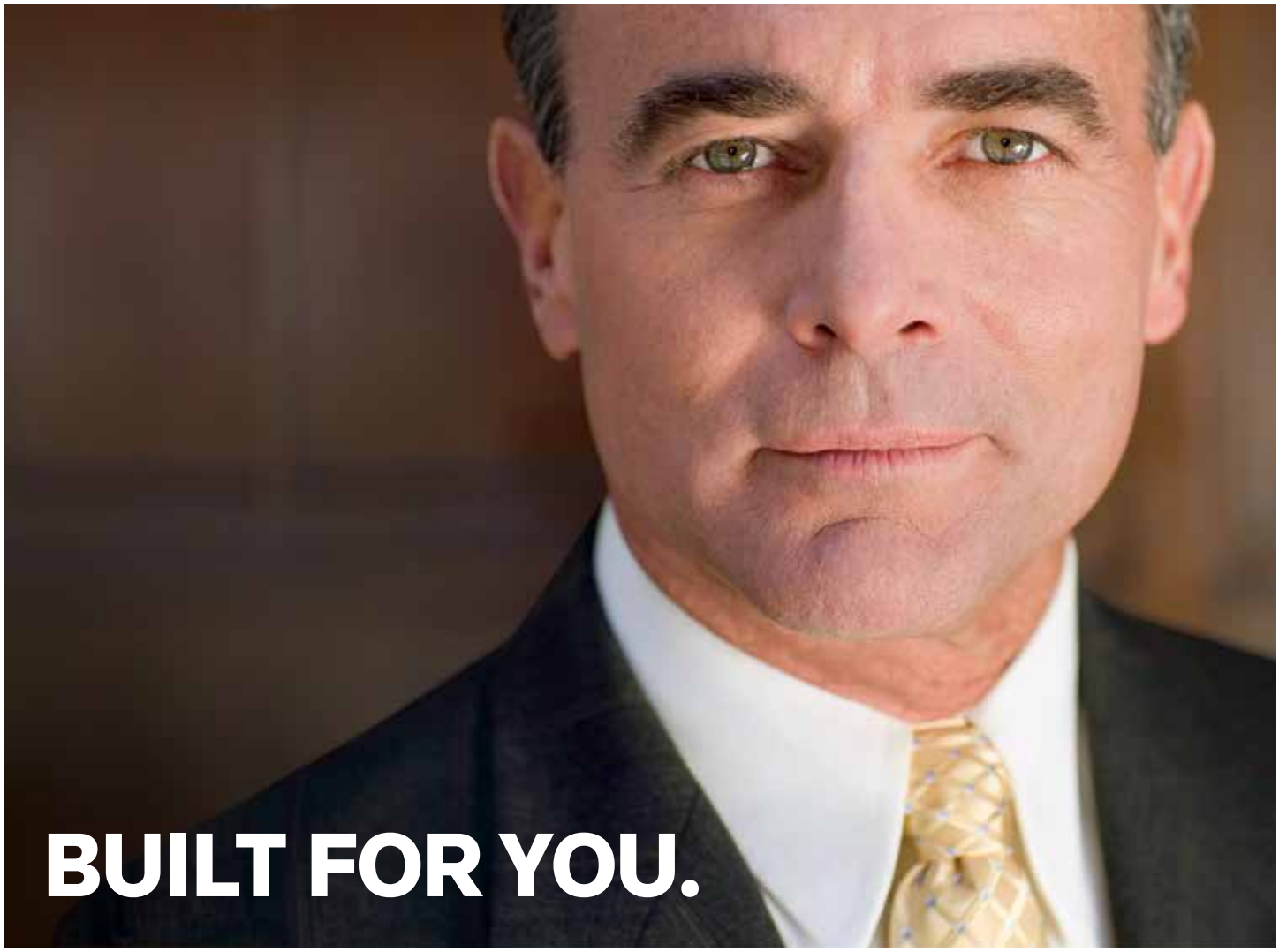
Esto llega a la imprenta cuando ACAMS ha tenido varias reuniones preliminares de profesionales de ALD, representantes de aplicación de la ley y expertos de delitos financieros, todos los cuales han confirmado nuestra perspectiva sobre esta nueva certificación — que es necesaria para los que tienen experiencia para aumentar su capacidad pericial en este mundo desafiante de mantenerse por delante de los actos de los delincuentes, terroristas y otros estafadores. Nuestra primera escuela comenzará en enero de 2014 y habrá mucho más en este esfuerzo innovador para ampliar el estándar de ACAMS a la área importante de investigaciones financieras avanzadas.

Ustedes no encontrarán propaganda o marketing de la más alta categoría en este esfuerzo, sólo los valores de ACAMS que ustedes. nos exigen y esperan de nosotros.

Finalmente, quiero agradecerles a todos los miembros de los grupos de aplicación de la ley por su trabajo constante en mantenernos seguros y erradicar a los delincuentes.



John J. Byrne, CAMS
vicepresidente ejecutivo



A NEW INVESTIGATIVE PLATFORM: CLEAR® FOR ENHANCED DUE DILIGENCE

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

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

Visit clear.thomsonreuters.com to download our new white paper on anti-money laundering.

THOMSON REUTERS™

Karen O'Brien, CAMS:

La disponibilidad de fondos frecuentemente hacen que un caso tenga éxito o fracase

Karen O'Brien es la dueña actual de Global Compliance Solutions, una compañía dedicada a ayudar a las empresas con el cumplimiento del antilavado de dinero. Antes, fue un oficial de policía del servicio de Policía de Toronto por 16 años, de los que durante los últimos cinco los pasó como sargento del Escuadrón de Fraude y Falsificación. También pasó dos años investigando delitos financieros en las Islas Caimán con la Real Policía de las Islas Caimán. También es una Especialista Certificada en Antilavado de Dinero.

ACAMS Today: Usted pasó más de 16 años como investigadora. ¿Nos podría hablar sobre su investigación más memorable de lavado de dinero?

Karen O'Brien: La que me viene a la mente es el caso de las Islas Caimán en la que me involucré. No fue el de mayor éxito, desde la perspectiva de las acciones judiciales, pero de la perspectiva de la víctima tuvo éxito porque los fondos se recobraron y fueron devueltos. Fue un caso clásico de estratificación. Involucró una transferencia por cable fraudulenta, por medio de instrucciones cableadas por escrito que fueron entregadas al banco y falsificadas de una empresa manejada desde las Islas Caimán. El dinero fue transferido desde las Islas Caimán a Atlanta, Georgia y de ahí a Edinburgo, Escocia y luego hubo un intento de enviarlo a Dublín. Una vez que se descubrió el fraude, que, convenientemente, ocurrió alrededor de la Navidad — justo entre Navidad y Año Nuevo — período durante el cual la mayor parte de las empresas y bancos están a media marcha o se encuentran cerrados para las fiestas. Creo que se planificó así estratégicamente. Creo que los delincuentes pensaron que para cuando nos diéramos cuenta de la manipulación de los fondos, ya estarían en Irlanda o en algún otro lugar. Pero logramos ponernos al día con los fondos en Escocia antes de que se pudiera ejecutar la transferencia a Irlanda.

El caso fue memorable porque el individuo que trató de transferir los fondos de Escocia a Irlanda anotó mal el número de la cuenta porque estaba borracho cuando entró al banco. Así que fueron devueltos.

Aunque identificamos a los individuos involucrados en el caso, el gobierno de las Islas Caimán prefirió no extraditarlos porque el costo era demasiado alto. Así que recuperar el dinero fue un éxito en algunos aspectos. Pero los individuos nunca fueron llevados a juicio por los delitos.

AT: ¿Es a menudo un problema?

KO: ¿Qué la gente esté borracha cuando trata de delinquir?

AT: [Risas.] Lo que quería preguntar ¿es la falta de fondos un problema común cuando se investigan y juzgan delitos financieros?

KO: Sí, y no se limita a las Islas Caimán. El dinero es un tema dondequiera y siempre se oye en las noticias que se reducen los presupuestos. Hubo otro caso en el que un compañero y yo tuvimos que ir a Turcos y Caicos para una investigación de robo electrónico de tarjetas de crédito. Se trataba de un caso grande pero los fondos no estaban allí y el servicio de policía simplemente no podía cubrir los costos de continuar investigando. Así que los fondos son una cosa importante. Las investigaciones financieras pueden ser muy caras, especialmente cuando cruzan las fronteras, y la mayoría lo hacen hoy día.

AT: ¿Qué cosas pueden hacer los investigadores para vencer los desafíos que involucran las investigaciones transfronterizas?

KO: Lo primero que tenemos que hacer es conseguir la cooperación de la jurisdicción involucrada y generalmente no es problema. Pero hay algunos protocolos y cierta burocracia que hay que seguir antes de empezar a hacer las cosas. Frecuentemente hay que confiar la investigación a otros y esperar que se ocupen. Hay prioridades diferentes para jurisdicciones diferentes, y con recursos limitados, las jurisdicciones sólo pueden hacer lo que les permite sus presupuestos. Es un desafío difícil. La cooperación está ahí. Existen memorandos de entendimiento que ayudan en las investigaciones transfronterizas. Pero el tema no es ese. Nuevamente, es un tema de finanzas, recursos y desafortunadamente a veces hay que tomar una decisión sobre hasta dónde se va a llegar con algo. Como en el caso descrito antes, conseguir los fondos para la víctima, consideradas las circunstancias, fue lo mejor que pudimos hacer.

AT: También investigó casos en jurisdicciones secretas offshore tales como las Islas Caimán y la Isla de Man. Estas regiones han estado recibiendo escrutinio mundial por prácticas de secreto bancario. ¿Están exagerados los riesgos asociados con estas jurisdicciones?

KO: En absoluto, no puedo insistir bastante sobre esto. A través de los años se han armado mecanismos, tales como acuerdos de intercambio de información impositiva, el uso de memorandos de entendimiento de investigaciones financieras y otras herramientas que ayudan en las investigaciones transnacionales. Hay un gran malentendido acerca de las herramientas disponibles para recoger información en otras jurisdicciones.

AT: ¿Puede listar unas tendencias actuales de lavado de dinero?

KO: Creo que una de las grandes tendencias que nos tienen que preocupar es el uso de empresas offshore. Necesitamos legislación que requiera identificar los dueños beneficiarios y tiene que ser más coherente a través de las jurisdicciones. Esa fue una de las recomendaciones revisadas de FATF del año pasado. Pero aún falta armonizarla en todas las jurisdicciones por lo que hay discrepancias. Los delincuentes siguen usando estas empresas para abrir cuentas bancarias, para tratar de enviar dinero de jurisdicción a

jurisdicción y saben que una vez que cruza la frontera la investigación se hace más desafiante debido a finanzas y recursos.

El blanqueo de dinero mediante operaciones comerciales es otro tema porque el tamaño de la industria mundialmente es tan vasto. Es una industria difícil de controlar y examinar como quisiéramos porque sencillamente es demasiado grande.

Pero las tendencias por las que tenemos que preocuparnos son las que no hemos identificado todavía, porque si las conocemos entonces los delincuentes las conocen, lo que quiere decir que pasan a otro tema.

AT: Los riesgos de blanqueo de dinero por medio de tarjetas prepagas han estado en los titulares durante años. ¿Hay pruebas de que las explotan los delincuentes?

KO: Sí, las hay. Hubo un caso en particular en Dubai en enero de 2010. Había una asignación a un individuo con lazos militantes y se encontró que 14 de los 26 sospechosos habían usado tarjetas prepagas para cubrir sus gastos de hotel y otras cosas. Ese es sólo un ejemplo. El gobierno y los legisladores de EE. UU. no se ocuparían tanto de ello si no fuera un problema.

AT: ¿Qué me dice de los juegos virtuales, monedas y Bitcoin?

KO: Los investigadores que tienen las destrezas de investigar el blanqueo de dinero por medio de las monedas virtuales o por medio de Internet son pocos. Toma cierta habilidad, y muchas jurisdicciones ni siquiera tienen regulaciones sobre las monedas virtuales, a pesar de que constituyen una tendencia emergente. Por de pronto, esta es una preocupación grande. Los Estados Unidos tienen buena legislación sobre las monedas electrónicas. Pero todo el mundo está tratando de ponerse al día y ya existía antes de que apareciera la legislación.

AT: Usted ahora trabaja de consultora. ¿Cuáles son los desafíos de cumplimiento que los oficiales del ramo se encuentran en el día a día?

KO: Lo mayor es que el cumplimiento excede el ALD. Ha evolucionado tanto en los últimos 10 a 12 años y todos los oficiales que veo y con quienes hablo tienen mucho más que hacer ahora, y se espera que hagan más con menos recursos. También se espera de ellos que sean expertos reguladores en sus propias jurisdicciones y expertos en otras jurisdicciones. Así que el papel del oficial de cumplimiento evoluciona más allá de un conjunto determinado de destrezas.

AT: ¿Qué tendrían que hacer los oficiales de cumplimiento para combatir estos desafíos? ¿Tendrían que fusionarse los departamentos para utilizar recursos?

KO: Van a fusionar los departamentos para ahorrar. No hay nada que podamos hacer en cuanto a eso. En algunas organizaciones funciona y en otras no. Depende de la estructura de la organización. Lo que importa es la diversidad y el entrenamiento cruzado. Hace falta expandir la base de conocimiento; no hay que tener un oficial único de cumplimiento con experiencia que asiste a todas las conferencias y cursos de entrenamiento. Tiene que haber capacitación diversa entre los miembros del personal para que no sólo sea una persona la que sea experta en todo. El departamento de cumplimiento tiene que trabajar al frente de la casa — el lado operativo del negocio y el cliente que enfrenta al personal. Tienen que trabajar conjuntamente y no en oposición, ya que el cumplimiento siempre se ve como inhibidor del crecimiento comercial. No habría que verlo así. Tendrían que trabajar conjuntamente para identificar los riesgos y mitigar estos riesgos antes que impedir hacer negocios.

AT: ¿Qué cosa única, la cosa más importante que puede hacer un oficial de cumplimiento para impedir el lavado de dinero?

KO: Es importante hacer el trabajo lo mejor posible. Honradamente, el lavado de dinero no va a desaparecer. Los delincuentes van a cometer crímenes y necesitan blanquear su dinero. Pero tenemos que poner de nuestra parte para gestionar los riesgos que podamos — manejando nuestra propia oficina o empresa. Eso es todo lo que podemos controlar así que necesitamos manejar estos riesgos internos lo mejor posible.

Entrevista por: Larissa Bernardes, editora de web de ACAMS moneylaundering.com ACAMS, Miami, FL, EE. UU., lbernardes@acams.org

Lunes, Lunes, no puedes confiar en ese día...

Posiblemente, las *Mamas & los Papas* no tenían en mente la Ley Antilavado de Dinero (ALD) cuando cantaban sobre el lunes, pero el primer día hábil de la semana es un día problemático para quienes están involucrados en investigaciones antilavado. "¿Dónde estaba usted el [insertar día/hora]?" es la pregunta más habitual en el trabajo detectivesco. Lamentablemente, las entidades financieras no se solidarizan con la obsesión de los investigadores por diferenciar "a tal hora" de "*alrededor* de tal hora". Para los investigadores, las coartadas no están sujetas a la "flotación". Las entidades financieras — y una buena cantidad de los defraudadores, para el caso — viven y mueren por la flotación. Los investigadores antilavado pronto descubren que, en cuestiones relacionadas con la banca, no se puede confiar en el lunes.

Los investigadores siguen calendarios precisos y sincronizan sus relojes. Por lo pronto, fue su pensamiento orientado a los detalles lo que los llevó a ejercer esa profesión. Por más orientadas a los resultados que puedan parecer las entidades financieras en otras cuestiones, su calendario frecuentemente queda abierto a la interpretación. En su mundo, el lunes empieza en algún momento de la tarde del viernes. Durante su semana, el próximo día empieza — por rutina — en la tarde anterior. Los escaneos, los sellados y las impresiones que ocurren detrás del mostrador del banco el viernes por la tarde ya han sido remitidos al lunes. Los documentos, que incluyen su próximo estado de cuenta, reflejarán esas transacciones como si se hubieran efectivamente completado el lunes. Las entidades financieras operan con calendarios que sólo tienen "días hábiles", que no reconocen sábados, domingos o feriados. Ese concepto se profundiza mediante el efectivo corrimiento del tradicional "cierre del negocio" de la semana a una hora tan temprana como las 14.00.

Los investigadores ALD usan "días hábiles" para las órdenes judiciales u otras cronologías legales pero suelen no reconocer sus implicancias en el análisis de una investigación ALD. El día real y la hora real en que los delincuentes practican sus acciones infames tiene gran importancia en esos casos. Para todo análisis hay que poder pensar fuera del casillero "día hábil".

Actualmente, no es raro que un negocio opere los siete días de la semana o que haga depósitos en forma diaria. Esto puede incluir la noche del viernes y algunos depósitos del fin de semana. Cuando el propietario de la empresa va a la entidad financiera el lunes, puede encontrarse con que fueron acreditados dos o más depósitos en su cuenta ese día. Incluso, puede que esos depósitos de sábado y domingo se estén registrando simultáneamente en otro cajero, mientras él está en el banco haciendo otra transacción el lunes por la mañana. En realidad, el depósito del viernes a la tarde puede aparecer como el último y no como el primero de la serie de depósitos del fin de semana. La cuenta de los días avanza pero el sello fechador, no.

Los departamentos de citación judicial sólo suelen copiar y reimprimir la documentación que refleja el día hábil al que la transacción es atribuida. Ese no es siempre el día y la hora en que la persona investigada estuvo físicamente en la entidad financiera. Esa información no es importante para los propósitos del negocio, pero puede ser crucial para los propósitos investigativos. Los investigadores deben reconocer que esa documentación aparentemente contradictoria, por más orientada a los detalles que parezca, no fue diseñada con propósitos de investigación en mente.

Los únicos documentos que, con mediana precisión, reflejan cuándo un cliente estuvo en una entidad financiera son los registros diarios de los cajeros. Hoy en día, estos suelen ser mayormente anotaciones electrónicas a las que los oficiales de citación judicial no pueden acceder con facilidad. Muchos de esos registros tienen un formateo único o codificación que puede requerir ayuda del banco para descifrarlos. "Frustración" no es un lamento raro entre los investigadores que tratan de obtenerlos.

También está el problema de manejar los depósitos nocturnos, las bolsas de depósitos comerciales y el surgimiento de la banca electrónica. Si bien los cajeros conocen y comprenden esto, muchos investigadores antilavado omiten dar cuenta de esos elementos cuando analizan transacciones sospechosas. Lo cierto es que, llegado el lunes, puede haber mucha actividad atribuida a ese día pero que no se realizó en su transcurso. Cualquier investigación antilavado que no tenga en cuenta esa deformación respecto de los "días hábiles" será inexacta y engañosa. El problema más serio es que esto lleva a que más actividad no sospechosa sea calificada como sospechosa y viceversa.

Una empresa que hace depósitos diariamente puede encontrarse con que una acumulación de depósitos en efectivo atribuidas al mismo día puede ser lo suficientemente grande como para despertar alertas, y quizás un SAR (Suspicious Activity Report/Informe de Actividad Sospechosa). Dos o más depósitos hechos en el mismo día con indicación de que fueron demasiado próximos entre sí — respecto de las prácticas habituales de negocios — pueden funcionar como disparador de una revisión antilavado. Sin embargo, si uno considera las acciones en tiempo real y encuentra que, en realidad, esas transacciones se extendieron a lo largo de todo el fin de semana, la revisión antilavado puede no ser necesaria. Incluso, después de que se presenta un SAR y un investigador recoge y revisa los back ups, puede ser que los documentos revisados reflejen múltiples depósitos en un mismo día, en el que quizás no se hicieron. Es raro poder acceder a las entradas de los registros diarios con un pedido de investigación inicial, ya se trate de back ups de documentos SAR o de una citación judicial. También debe señalarse que los tickets de depósito y la impresión de la fecha reflejarán solamente un mes y un día. Para saber qué día de la semana era, hay que ir a buscarlo en un calendario. Mucho tiempo y sustanciales esfuerzos de investigación pueden desperdiciarse antes de que la "anomalía lunes" pueda ser por fin reconocida.

La excelencia en las investigaciones antilavado requieren que cuestionemos todo y que aprendamos sobre los muchos elementos distintos de los mundos financiero y criminal. Los números y los dólares son muy ambivalentes y sólo determinan su relevancia las personas que están detrás de ellos. Las transacciones bancarias se vuelven ilegales cuando se vinculan con ellas ciertos elementos externos. A pesar de que delitos como la falsificación, la falsificación de documentos y la utilización de documentos apócrifos son delitos propios de las transacciones; el lavado de dinero responde más comúnmente a un esquema de transacciones múltiples, por lo que hace falta conocer la totalidad de las transacciones y otros eventos para dejar expuesto su carácter delictivo. Tener pericia en la investigación antilavado requiere un profundo análisis de todos los aspectos de tales transacciones. Todo lo que el sujeto hizo (y cuándo) o no hizo, y todo lo que la entidad financiera hizo (y cuándo) o no hizo, es relevante hasta que la investigación haya llegado a la conclusión de que no lo es.

Hoy en día, nuestras actividades quedan mucho más documentadas que antes. Nuestros celulares y GPS pueden decir dónde estamos o dónde estuvimos. Los mensajes de texto y los correos electrónicos memorizan conversaciones o pensamientos que muchas veces querríamos fueran borrados. Nuestros automóviles tienen "cajas negras". Todos esos datos pueden ser valiosos para los investigadores siempre y cuando se recuerde que mucha de esa información fue recogida sin tener en cuenta las necesidades de la investigación. Interpretar la relevancia investigativa es parte del trabajo. Por cierto, los registros de las entidades financieras son algo de lo que los investigadores antilavado deberían estar fuertemente conscientes.

Una vez que un investigador antilavado descubre que no se puede confiar en el lunes, va a poder apreciar mejor los fines de semana.

Steve Gurdak, CAMS, supervisor, Washington Baltimore HIDTA, Northern Virginia Financial Initiative (NVFI) Annandale, VA, USA, sgurdak@wb.hidta.org

Después de la presentación:

Análisis del SAR desde el punto de vista de los que aplican la ley

En algún lugar secreto cerca de Washington D.C., un equipo de analistas de aplicación de la ley está revisando informes de actividad sospechosa (SAR en inglés). Como rutina los grupos de tareas en todo el país se reúnen para discutir de y revisar las presentaciones de SAR, y los departamentos de policía lugareños también pueden estar revisando el SAR que usted presentó recientemente. Han pasado los días en los que los bancos y los representantes de la ley estaban en desacuerdo sobre la importancia de tal información y si se usaba. Usted puede estar seguro de que esta información se usa de manera amplia.

Pero ¿qué busca el representante de la ley? La respuesta habitual es "depende". Esa es una descripción tan acertada como puede ser. Depende de la destreza y experiencia del analista, la motivación del redactor y del investigador, y de muchas otras variables. Lo que se sabe es que su presentación del SAR la recibe la Red de Aplicación de Delitos Financieros (FinCEN en inglés) y luego desde varios puntos de acceso se la redirige para investigar por parte de los representantes de la ley.

Así como hay un propósito y un método para redactar un buen SAR, también hay buenas maneras de analizar e interpretar un SAR. En lo que sigue de este artículo se describirá lo que buscan los representantes de la ley y esto, a su vez, les dirá algo a los que presentan un SAR.

Todos los SAR son buenos

El primer concepto importante es que no hay presentaciones malas de SAR — sólo que algunas son mejores que otras. Los que aplican la ley están acostumbrados a recibir información conflictiva, información parcial, enunciados captados en un momento de emoción y claras mentiras. Los representantes de la ley están equipados y tienen experiencia para buscar la verdad y para conseguir los detalles que son importantes.

Las presentaciones de SAR son informes escritos de pistas que se pueden explotar para desarrollarlas, y los detalles son de la mayor importancia. Los de la ley aprecian todas las presentaciones de SAR. Ningún detalle es demasiado pequeño para no incluirlo en una narración de SAR. Cierto es que el quién, qué, dónde, cuándo, por qué y cómo debería guiar al redactor del SAR para que añada detalles de los involucrados, tales como sus documento de identidad, empleo, la línea de tiempo de los hechos, sumas involucradas y, de manera más importante, lo que sospecha el redactor que puede estar pasando.

Es importante reconocer que la aplicación de la ley no entiende los negocios y el comercio de la manera como lo hace una institución financiera. El autor de un SAR tendría que conocer a su cliente y poder dar información en la narrativa del SAR acerca de los negocios del sospechoso. La ley siempre tendrá que revisar el SAR desde la perspectiva del autor. Sea usted buen informante dando el contexto de negocio si se necesita explicar lo que puede ser un negocio normal y por qué la actividad sospechada se desvía de la norma.

Muchos SAR puede ser mejor

Presentaciones múltiples de SAR ocurren naturalmente cuando el sospechoso de un banco o de un negocio de servicios de dinero (MSB en inglés) continúa con actividad sospechosa y el banco o MSB elige presentar un nuevo SAR al mes siguiente o al que le sigue. Estas presentaciones se toman en cuenta por lo que son, actividades consecutivas generalmente del mismo patrón, llevado adelante en varios meses, y generalmente por los mismos. Los de la ley revisan estos tipos de SAR y luego calculan la actividad mensual (u otra frecuencia), y después trabajan para sumar la actividad total. Estas presentaciones múltiples son importantes para el oficial de aplicación de la ley, pero a veces se

hacen una "rutina" sin información nueva más que el cambio de fecha de presentación y las cifras de dinero.

Lo que puede ser de mayor valor e importancia para los de la ley son los hallazgos de más SAR presentados por otros bancos sobre el mismo sospechoso o grupo de sospechosos. Estos SAR adicionales, permiten al investigador ver múltiples perspectivas de actividad sospechosa que han podido ocurrir en los bancos u otras instituciones financieras. Además, estas presentaciones múltiples permiten que el investigador reciba opiniones expertas de dos o más oficiales de ALD quienes saben lo que es normal para un negocio. Esta información es de tremendo valor para el oficial de aplicación de la ley quien tal vez no sepa del negocio o de la industria.

¿Qué mira primero el que aplica la ley?

El oficial de aplicación de la ley también mirará el SAR para ver si otras agencias han sido contactadas. Dos oficiales de la ley o más que trabajan sobre el mismo caso pueden traer más sinergia a la investigación total.

El oficial de aplicación de la ley también mira "entre líneas" del SAR para determinar si las cuentas fueron cerradas, la duración de la actividad antes de cerrar la cuenta, y la duración de tiempo antes de establecer nuevas relaciones de negocios con un banco nuevo. La apertura y el cierre de cuentas en proximidad a áreas geográficas normales de residencia o de trabajo se revisarán también.

Los que aplican la ley tienen que cumplir con dos cosas cuando miran un SAR. La primera es desarrollar una teoría potencial relativa a la trama delictiva que se informa. La segunda es el desarrollo de una metodología o plan para conducir la investigación que tiene entre manos.

Los que aplican la ley empiezan el análisis

Con estas ideas en mente, el oficial de aplicación de la ley puede empezar su investigación y determinará el orden y los pasos para conducir la investigación. Es importante que el representante de la ley no llegue a conclusiones apresuradas, y ciertamente no es aceptable no entender por completo el SAR al inicio de la investigación. Lo que es importante es que el desarrollo de la trama delincuencial potencial sea desprejuiciada, fluida, y que se pueda cambiar, re-enfocar y re-examinar durante la investigación.

El representante de la ley puede no entender la narrativa del SAR que usted ha escrito al comienzo, a pesar de sus mejores esfuerzos para simplificarla o explicar el tema. Intentará relatar lo que se dice obviamente en el SAR y tratará de que tenga sentido. A pesar de su formateo, columnas, tabulaciones y otras formas de editar, todo puede perderse entre el procesamiento en su banco y de última lo que el de la ley pueda ver en su computadora. Con suerte, si el tema es de naturaleza técnica, la narrativa del SAR lo desmenuzará en piezas más pequeñas, de más fácil comprensión.

A veces el investigador tendrá que copiar y pegar todo el SAR en un documento de Word. El investigador que usa este método añadirá cortes personalizados de párrafos para determinar temas mayores que ocurren en la narrativa del SAR. Los temas comunes pueden enfocar tiempos, eventos, cantidades o fechas. Esto mejorará en gran parte las oportunidades de contestar a la pregunta: ¿Qué pasa?

Entendiendo el SAR

Superando el golpe inicial sobre la magnitud de la trama, complejidad del negocio o de la industria u otros bloqueos mentales será más fácil para que el que aplica la ley entienda revisando pequeñas porciones de la información de SAR. ¿Todo esto fue entrada de efectivo? ¿Hay efectivo o cheques correspondientes que salen? ¿Hay un balance de depósitos y retiros? ¿Dónde va el dinero? ¿A quién le llega? ¿Con cuánta frecuencia? Trazar un simple diagrama ¿ayudará a mostrar lo que está pasando? ¿Hay empleados que sean testigos? ¿Alguien en la industria puede ayudar a explicar cómo uno de estos negocios normales puede funcionar legalmente? ¿En qué difiere este? ¿En qué es igual? La lógica comparativa y contrastiva puede ser un aliado de los investigadores en esta etapa de revisión.

Todos necesitan tomar una pausa mental en este punto. Muchas investigaciones no descubren la verdadera extensión de lo que ha ocurrido hasta completar el caso y aun entonces parece que siempre existe "el que se escapó" (o que estaba involucrado pero contra quien no se pueden entablar acciones judiciales por falta de pruebas suficientes). En esta etapa temprana, los analistas e investigadores no sólo intentan ver si el SAR coincide con otro SAR o caso con el que han estado involucrados. Las direcciones del efectivo, los cheques y los giros ¿son similares? Otra persona en su oficina o región ¿tenía un caso o una investigación que involucró este tipo específico de giros? ¿Han oído hablar o visto otra trama similar en otra área geográfica? ¿Leyeron algo en ACAMS sobre este tipo de estafa o la están viendo por primera vez?

Comienza la investigación

Re-contactar la institución financiera para verificar la información del SAR es siempre un paso clave para el investigador inteligente. Un banco o negocio de servicio de dinero será una riqueza de conocimiento en cuanto al SAR y la actividad que se describe. Otros departamentos o áreas de una institución financiera tendrán que considerarse para posibles citaciones para encontrar tales cosas como documentos de préstamos, cajas de seguridad o tal vez inversiones.

Socios de negocios, cónyuges, novios, novias pueden pronto encontrar que son testigos de la investigación y ellos a su vez tendrán su información re-vista a través de las bases de datos investigativas (incluyendo las verificaciones de datos de BSA) para hacer evaluaciones iniciales por si se encuentran o no involucrados o deben considerarse como testigos. Los hallazgos de SAR adicionales y documentos de BSA pueden llevar al investigador a demorar contactos iniciales con sospechosos principales y ampliar la investigación.

En esta etapa, una búsqueda completa de todos los documentos de BSA tendría que conducirse antes de que empiecen las actividades de campo. Tener ejemplos de información de BSA anteriores ayuda a los investigadores a preparar preguntas, y pueden usarse como medida para validar respuestas. Frecuentemente en la fase de interrogaciones los que aplican la ley obtienen una confesión basada en una comprensión completa y abarcadora de todos estos hechos. La verdad no miente.

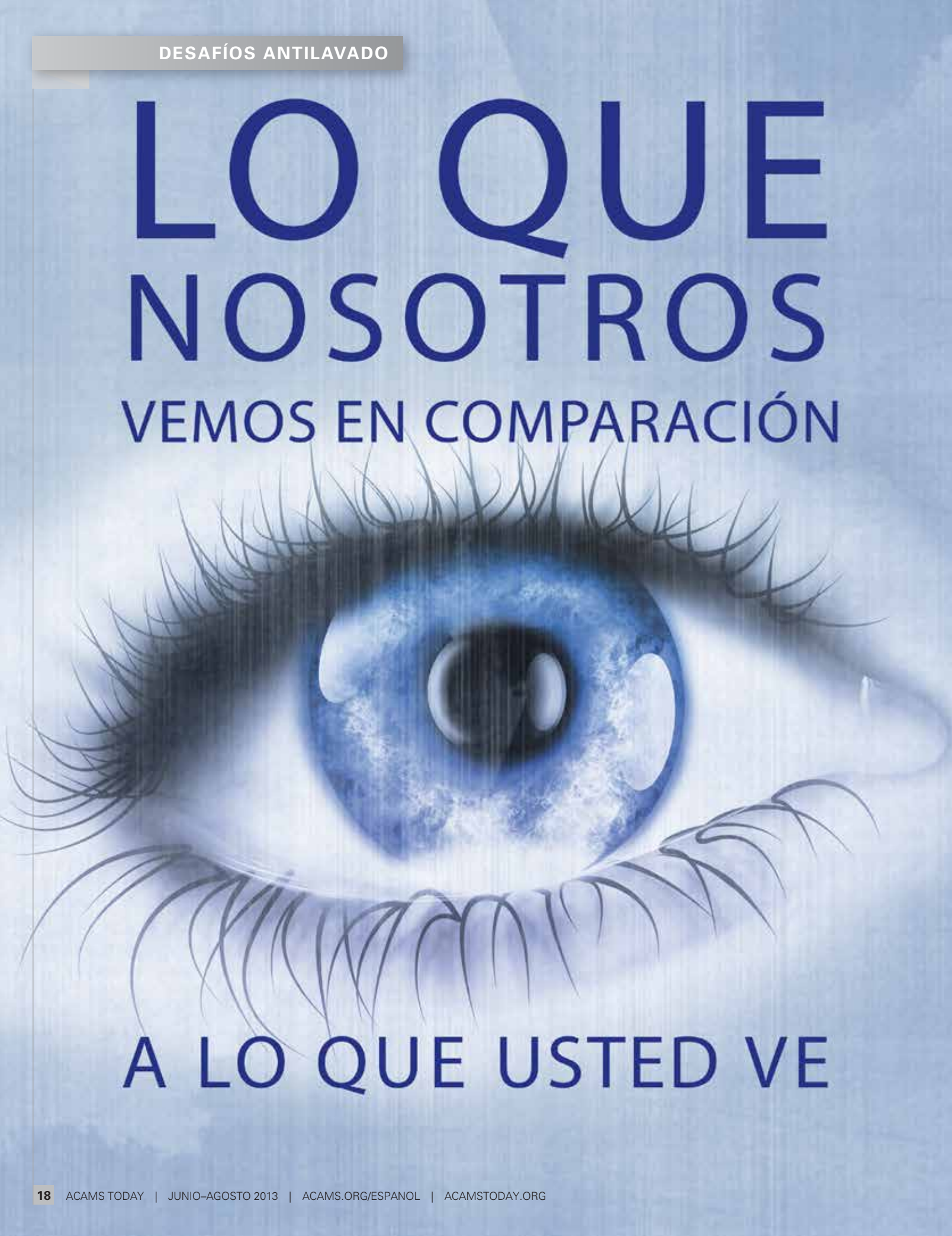
La investigación continúa

En conclusión, el SAR es sólo una pista. Se necesitará mucho trabajo adicional para evaluar adecuadamente la información en relación a otras piezas de prueba a medida que progresa la investigación. La presentación de un SAR solo nunca es prueba *prima facie* de un delito ya que el SAR no puede divulgarse; sin embargo, es el análisis cuidadoso de la información del SAR en conjunción con otros elementos que llevan a los que aplican la ley a enjuiciamientos exitosos.

La asociación de la industria financiera y de la aplicación de la ley es importante y sigue en crecimiento. Los delitos financieros se están haciendo extremadamente complejos. Tener la industria financiera en la primera línea para ayudar a los que aplican la ley para que identifiquen estos delitos será clave para proteger nuestro sistema financiero y futuro financiero mutuo.

Erick Malette, CAMS, CFE, contratista del gobierno, cliente antes trabajó como agente especial del Departamento de Tesorería de los Estados Unidos, erick.malette@cox.net

LO QUE NOSOTROS VEMOS EN COMPARACIÓN



A LO QUE USTED VE

En las primeras horas de la mañana, en un tranquilo vecindario, unos fuertes golpes en la puerta principal despiertan al propietario de una casa. Cuando éste abre la puerta, se encuentra con un joven que está sangrando profusamente en su umbral. Se hace un llamado al 911 y se envían oficiales de policía. Una vez llegados al lugar, uno de ellos habla con la víctima, quien declara sobre un robo que sufrieron tres hombres que estaban adentro de la casa de enfrente. La investigación subsiguiente revela que los dos hombres asaltados habían sido torturados y asesinados. El joven ensangrentado era el tercero de ellos. Él también había sido torturado, y murió después de declarar que se trató de un robo de drogas que salió mal. Se describe que la escena es horrible.

Esta triste historia ocurrió en el Condado de Fairfax, Virginia, y lamentablemente ocurren muchas historias similares en Estados Unidos y en todo el mundo. Lo que ven las entidades financieras es el principio de este drama. Un individuo entra en una entidad financiera o una empresa de servicios monetarios y gira dinero desde la costa este a la costa oeste. Ese mismo individuo va a dos o tres otras empresas y gira la misma cantidad a la misma cuenta bancaria. Otro individuo en la costa oeste extraerá los dineros enviados y, entonces, se enviará un cargamento de marihuana u otras drogas ilegales a la costa este por UPS, Fed-Ex, el Servicio Postal de los EE.UU, Mail Boxes, etc. o cualquier otro servicio de envío. Si el cargamento no es interceptado por las autoridades, el distribuidor de droga ya estará haciendo su negocio.

Los individuos que lavan dinero a través de entidades financieras no suelen ser delincuentes violentos. Sin embargo, esos dineros cargan con crímenes violentos en su historia. Un juicio que está teniendo lugar ahora en Texas involucra a un cartel de drogas mexicano que lavaba ganancias hechas con los caballos. Esto es lo que ve el público y lo que ven las entidades financieras. Son los agentes de la ley quienes ven los homicidios sin sentido atribuidos a la venta ilegal de drogas en todo el mundo.

Un caballero entra en un salón de masajes y paga cierta cantidad por un masaje, usando su tarjeta de crédito. Pocos minutos después, la tarjeta se usa para una segunda transacción. El importe es mucho más alto que el de la primera. ¿Esto le resulta sospechoso? Para las autoridades, esto se reconoce como posible prostitución. Lo que usted ve como entidad financiera es la utilización de la tarjeta de crédito para pagar servicios. Lo que las autoridades ven es una mujer, adulta o menor, víctima del negocio de esclavitud sexual. La primera lectura de la tarjeta de crédito es para el supuesto masaje legítimo. Comúnmente, la segunda lectura es para servicios sexuales ilegales.

> La mayoría de la gente siempre está feliz con su vida cuando nada interrumpa su rutina diaria

Estos son los tipos de casos que a veces quedan sin detectar ni denunciar. Son los casos más grandes los que suelen denunciarse a la Red de Cumplimiento contra los Delitos Financieros (FinCEN, por sus siglas en inglés), a través de la presentación de Informes de Actividades Sospechosas (SAR, por sus siglas en inglés).

Una persona entra en una entidad financiera para depositar cuatro mil dólares en su cuenta de ahorro. El cajero recibe el efectivo e inmediatamente detecta un fuerte olor a marihuana que emana de los billetes. El cajero conoce el olor de la marihuana por experiencia de vida. El cajero decide no denunciar la transacción como sospechosa por temor de las repercusiones de tener que responder preguntas sobre por qué conoce el olor de la marihuana. Esto ocurre más a menudo de lo que usted pueda pensar.

Un individuo adquiere una tarjeta de efectivo prepaga y coloca dinero en ella. Ese individuo es un traficante de drogas. Alguien se contacta con él y hace un pedido. El traficante pide el código PIN que está en el dorso de la tarjeta. Luego va a un comerciante, le da el código PIN y recibe el efectivo de la tarjeta sin necesidad de tarjeta ni identificación. Entonces las drogas ilegales son enviadas al traficante y su negocio ilícito ya está operando.

Un individuo (jugador) hace apuestas ilegales con su corredor de apuestas. El jugador pierde constantemente a lo largo de la temporada. El jugador no tiene más dinero y está en la ruina. El corredor de apuestas ayuda al jugador a obtener un préstamo hipotecario para que pueda pagar sus deudas, legales e ilegales. Esta operación se hace con la ayuda de la novia del corredor de apuestas, que es una abogada especializada en bienes raíces. Al jugador le permiten nuevamente hacer apuestas, pierde nuevamente y queda en ruina financiera total. El corredor de apuestas y su novia ejecutan judicialmente la casa del jugador y, a través del sistema legal, desalojan al jugador y a su familia (esposa y dos niños).

Los medios muestran las escenas dramáticas públicas, fotos y videos de las escenas de crimen. Eso no es igual a estar en la escena. La mayoría de la gente siempre está feliz con su vida cuando nada interrumpa su rutina diaria. Se toma más conciencia de estos problemas cuando ocurre algo horrendo y la rutina diaria se destruye — como con los golpes en la puerta principal de su casa a la media noche. La muerte de un ser querido por sobredosis de droga, una hija obligada a entrar en el mundo de la esclavitud sexual, o una estafa que involucra donaciones para las víctimas de un gran evento traumático. La lista sigue y sigue.

En Texas, dos fiscales y la esposa de uno de ellos fueron asesinados recientemente. La investigación condujo a un contenedor de almacenamiento que contenía pruebas del crimen. El contenedor había sido alquilado bajo un nombre ficticio, así como el vehículo que se encontró en el mismo contenedor. El contenedor fue localizado gracias a la pista que proporcionó un amigo cercano del presunto asesino.

Theodore John Kaczynski (alias, el Unabomber) envió cartas-bomba hasta que fue capturado. Cuando esto ocurrió, tenía una carta-bomba ya construida y lista para enviar. Su captura se produjo gracias a un dato proporcionado por un familiar muy cercano: su hermano.

Es extremadamente difícil para un miembro de la familia o para un amigo de la familia presentarse a las autoridades y decirles que su ser querido o amigo puede ser capaz de asesinar. Sin embargo, piense solamente qué podría haber pasado si ellos no se lo hubieran dicho a las autoridades. ¿Es tan difícil notificar a las autoridades sobre un desconocido total que acaba de entrar en la entidad financiera a su cargo? Y si el evento no calificaba como para que su entidad elevara un Informe de Actividad Sospechosa, ¿qué le impide a usted llamar a las autoridades por su propia iniciativa, ya sea dando su nombre o de manera anónima?

La última tragedia nos recuerda algo que debería quedar grabado en nuestras mentes: "SI USTED VE ALGO, DIGA ALGO". Lo que usted ve debería ser lo que nosotros vemos, y juntos, entonces, quizás podamos contribuir a que se mejore.

James A. Cox III, CAMS, sergeant, Fairfax County Police Department, Fairfax, VA, USA, James.Cox@fairfaxcounty.gov

Deborah Morrisey, CAMS:

Siga el flujo del dinero

ACAMS Today tuvo la oportunidad de entrevistar a Deborah Morrisey, CAMS, la agente especial asistente encargada de Investigaciones Nacionales de Seguridad en Miami, Florida sobre su extensa carrera en investigaciones financieras.

Morrisey es jefa de equipo de cuatro grupos de investigadores que cubren todos los aspectos de investigaciones que enfocan delitos financieros transnacionales y lavado de dinero.

Se trata de una experta del tema (SME por las siglas en inglés) en investigaciones financieras y lavado de dinero nacionalmente reconocida, y frecuentemente se la convoca para revisar e informar o representar a ICE en reuniones nacionales y extranjeras; internacionalmente se la convoca para preparar artículos para la publicación e instruir a personal en el lavado de dinero.

Además, Morrisey ha cooperado en establecer y mantener asociaciones mixtas (públicas-privadas) internacionalmente con líderes financieros de la industria y profesionales de cumplimiento de la ley para promover esfuerzos efectivos contra el lavado de dinero y otros delitos financieros.

ACAMS Today: ¿Han aumentado los delitos financieros en los últimos cinco años? ¿Hay nuevas tendencias en los delitos financieros que no existían hace cinco años?

Deborah Morrisey: Los delitos financieros han aumentado y evolucionado durante los últimos cinco años. Es empíricamente difícil seguir los cambios en los delitos financieros. Algo que hemos visto es que las organizaciones típicas de bandas o de delitos callejeros han migrado al fraude financiero, tales como el robo de identidad y el fraude de telemarketing. Los crímenes financieros son más lucrativos y se perciben como menos riesgosos. Por ejemplo, en estos días se consigue más dinero robando la identidad de alguien que robando un banco pistola en mano.

Otra tendencia que estamos viendo es un gran incremento en el fraude identitario, tarjetas prepagas con dispositivos de acceso, tarjetas de crédito y fraude de reembolso de impuestos. Los delincuentes ahora se dedican a presentar declaraciones de impuestos para las identidades que han robado.

Algo que puedo decir empíricamente es que en los últimos cinco años los delincuentes financieros y lavadores de dinero se han hecho sustancialmente más sofisticados e internacionales.

AT: ¿Qué tipo de delito financiero es el que más investiga su agencia?

DM: Superviso el área de Miami-Dade pero específicamente la parte sur de Florida. Diría que el lavado de dinero basado en el comercio es a lo que dedicamos una buena parte de nuestros recursos. Tenemos todo un grupo dedicado a investigar el lavado de dinero basado en el comercio. También enfocamos delitos internacionales de corrupción pública y contrabando de dinero en efectivo. Nuestra autoridad para investigar delitos financieros y lavado de dinero es amplia. También investigamos fraudes financieros que cruzan las fronteras internacionales e intrigas que se centran en esconder los activos en casos de corrupción extranjera.

AT: ¿Nos puede hablar de cómo su departamento de investigación inicia un caso contra alguien que ha cometido un delito financiero?

DM: En realidad se trata de una pregunta difícil porque cada caso tiene una base de hechos diferente y un origen diferente. La manera de tomar nuestras decisiones al investigar depende de cómo se inició la investigación y de los hechos que conocemos. Por ejemplo, un proceso investigativo empezado cuando recibimos un informe de transacción sospechosa (STR en inglés) se gestionará de manera diferente que si recibimos la información de una fuente confidencial. Lo que puedo decir es que el denominador común que tienen todos los casos financieros consiste en seguir el flujo del dinero y conocer los detalles — seguir las transacciones.

También usamos todas las herramientas a nuestro alcance, sea analizar datos de la BSA, cultivar las fuentes de información o los testigos, acceder al ambiente físico o tomar los hechos en cuenta desde la A a la Z. Al final, el proceso de la investigación depende de qué tipo de delito se trata y de qué hechos están disponibles al empezar. Les decimos a nuestros investigadores que, cuando se investiga, hace falta ser tan creativo como los malos, pero asegurándose de que la creatividad cumple los parámetros legales.

AT: ¿Cuántos casos ha investigado respecto de la trata de personas y del contrabando de personas?

DM: Anoto las estadísticas de los casos iniciados, procesados, y los casos en los que ha habido un resultado positivo de arrestos en el año fiscal 2012:

Trata humana	2011	vs.	2012	
Casos iniciados	722		894	(+24%)
Arrestos	938		967	(+3%)
Acusaciones	444		559	(+26%)
Condenas	271		381	(+4%)
Confiscaciones	$2,054,459		$1,128,553	(–45%)

AT: ¿Qué pueden hacer las instituciones financieras en la lucha contra la trata de humanos y el contrabando de personas?

DM: En cuanto a las instituciones financieras, hay que recurrir a Conozca a Su Cliente. Incitamos a los bancos a que conozcan los indicadores de alarma (banderas rojas) para el tráfico humano tales como transferencias por cable que vienen de terceros o remitentes extranjeros, aberración en la actividad y tipo de cliente. Como en la mayor parte de las actividades delictivas, estar alerta es extremadamente importante.

AT: ¿Con cuánta frecuencia utilizan los narcotraficantes el sector financiero formal?

DM: Lo que resulta más riesgoso para los narcotraficantes es tener efectivo a mano porque es difícil de tener y de guardar. El resultado es que los narcotraficantes tratan de usar el sector financiero formal. Lo usan de maneras muy creativas para que entren sus fondos al sistema y para no parecer narcotraficantes. Una vez dentro del sistema financiero les resulta más fácil enmascarar y mover sus ganancias. Cuando se encuentran en el mercado negro o en grandes reservas de efectivo es cuando hay mayor riesgo para los narcotraficantes. Pienso que una de las cosas con las que podemos contar es que todos los delincuentes tratarán de usar el sistema financiero formal.

AT: ¿Qué tramas de blanqueo típicamente usan los narcotraficantes sudamericanos fuera del sector financiero formal?

DM: Fuera del sector financiero formal lo que más vemos aquí en el sur de Florida es el Intercambio del Peso del Mercado Negro (BMPE por sus siglas en inglés) porque ha sido usado y ha resultado desde el principio de los años noventas. Es un buen maridaje de lavado de dinero basado en el comercio y de un sistema financiero paralelo tanto para comerciantes legítimos como para narcotraficantes de lugares como Colombia. Este es el sistema financiero paralelo más común utilizado fuera del sector financiero formal. El otro es el contrabando de efectivo. Vemos que hay un flujo constante de dinero que se trafica sobre todo desde la frontera sudoeste de los Estados

Unidos. BMPE y el contrabando de efectivo son las dos tramas fueras del sector financiero formal que podemos ligar a los narcotraficantes.

AT: ¿Hay algo que pueden hacer las instituciones financieras para ayudar con las investigaciones aun cuando los delincuentes no usan el sector financiero formal?

DM: Sí, aun cuando los delincuentes no usan el sector financiero formal en un momento cualquiera, a la larga lo harán. Por ejemplo, un narcotraficante tiene efectivo en los Estados Unidos y el comerciante en Colombia va a usar sus pesos para comprar el efectivo que está en los Estados Unidos. Todo esto es informal, pero cuando el efectivo pasa a una transferencia por cable para pagar su envío de productos de una empresa de EE. UU. que va a Colombia, es cuando se recurre al sistema financiero formal. También, la meta del contrabando de efectivo es transferir el dinero al sistema financiero formal en algún punto débil dentro o fuera de los Estados Unidos, tales como pasarlo a una tarjeta prepaga o estructurándolo. Creo que el único sistema financiero paralelo que no toca el sistema financiero formal es el de Hawalas verdaderos.

AT: ¿Qué debe hacer un oficial de cumplimiento en el caso de que a él o ella lo amenaza un narcotraficante?

DM: Obviamente si es una amenaza inmediata necesitas llamar a los representantes de la ley o al servicio de emergencia instantáneamente. Si es una amenaza más velada, vas a tener que trabajar dentro de tus parámetros legales. Tendrás que hacer participar a los que aplican las leyes y ellos te dirán qué hacer.

AT: ¿Cómo han evolucionado las tramas de lavado de dinero de base comercial en los últimos cinco años?

DM: El cambio mayor de blanqueo de dinero de base comercial en los últimos cinco años ha sido la aparición de Venezuela y su mercado paralelo. Hay que comprobar que se tiene una deuda para sacar dinero de Venezuela, lo que crea incentivos para utilizar facturas falsas o facturas sobrevaluadas para ayudar a transferir fondos fuera del país. También, cuando los metales preciosos aumentan, resulta más fácil esconder mucho dinero. Es más fácil llevar una pequeña cantidad de metales preciosos para transferir valores de un lugar a otro.

Algo que se comentó en la conferencia de ACAMS en marzo respecto del lavado de dinero basado en el comercio fue que sólo hay un pequeño número de contenedores que se inspeccionan físicamente en la frontera. Una vez que los contenedores parten de la frontera (salgan o entren a los EE. UU.) puede empezar el debate sobre qué hay de verdad en el contenedor. Todo lo que tenemos son papeles. Cuando es todo lo que se tiene, hay vulnerabilidad para que las organizaciones delictivas alteren el valor de lo que de verdad estaba en el contenedor.

Mientras más contenedores inspeccionas más lento va el comercio, así que necesitamos una manera eficiente y efectiva de señalamiento inteligente. Una manera de hacerlo es la utilización de todo lo que se tiene disponible. Tenemos una Unidad de Transparencia Comercial en Washington, D.C, donde nos asociamos con nuestros contrapartes internacionales, incluyendo Argentina, Australia, Brasil, Colombia, Guatemala, Ecuador, Paraguay, México y Panamá para compartir nuestros datos comerciales. Algo que compartimos con nuestros socios es un gráfico de los datos que tenemos en un programa de computadora denominado darts ("dardos"). Este programa nos ayuda a identificar anomalías que aparecen en la lucha contra el lavado de dinero basado en el comercio.

AT: ¿Qué puede sugerir para que los sectores privados y públicos puedan aumentar su intercambio de información?

DM: Algo que hacemos es publicar un informe trimestral llamado Informe de piedra angular (Cornerstone report en inglés) (www.ice.gov/cornerstone). Así es como compartimos nuestras tipologías de caso e indicadores de alarma con el sector privado. También tratamos de asistir a tantas reuniones como podamos al nivel local. Tratamos de ir a las reuniones profesionales para mantener el diálogo entre los sectores público y privado tanto al nivel nacional como en nuestras oficinas externas.

AT: ¿Qué ha hecho su agencia para construir asociaciones en la lucha contra crímenes financieros?

DM: Asociarnos y tener asociaciones internacionales constituyen una de nuestras grandes prioridades, especialmente porque nuestras investigaciones son transfronterizas. Construimos las asociaciones en diferentes niveles.

1) Primero, tenemos presencia internacional en puntos clave en todo el globo (74 oficinas en 48 países), construimos relaciones con los representantes de la ley lugareños, desarrollamos fuentes y hacemos todo esfuerzo para trabajar cruzando fronteras en tiempo real de manera eficiente y efectiva.
2) Segundo, tenemos un programa grande de capacitación mutua con nuestros socios internacionales de aplicación de la ley. Esa capacitación internacional quiere decir que se envían instructores a países extranjeros y que instructores foráneos vienen a los EE. UU. para compartir ideas, investigar técnicas y estudios de casos.
3) En un nivel más alto, tenemos lo que llamamos Operation Firewall (Operación Cortafuego) en la que hacemos operaciones en tiempo real. Por ejemplo, si alguien sale de Miami y se dirige a otro país y declara $20,000 al salir, llamaríamos a nuestra contraparte en el otro país para prevenirlos de cuánto declaró la persona porque no se sabe cuánto declarará al llegar. También compartimos datos de aduana a través de Operación Cortafuego.
4) También trabajamos activamente con FATF, el Banco Mundial (Iniciativa de Recuperación de Activos Robados), Interpol y formamos parte de muchas directivas multinacionales y en el país somos parte del Grupo de Consultoría de BSA (BSAAG en inglés), Grupo de Tareas de Aplicación de Fraude Financiero y del Centro de servicios financieros para el análisis e intercambio de información.
5) Además, tenemos la Iniciativa de piedra angular (Cornerstone Initiative), que fue la que me trajo a ACAMS. La iniciativa hace que nuestros grupos hagan asociaciones públicas y privadas, abran esos diálogos para compartir lo que aprendemos de nuestras investigaciones con el sector privado y socios internacionales. Si no compartimos lo que aprendemos no le hace bien a nadie. También enviamos a nuestros empleados a participar como oradores en conferencias por todo el mundo y damos conferencias a otras agencias también. Construir estas asociaciones nos ayuda a trabajar efectivamente de manera informal aun antes de empezar los procesos formales.

Asociarnos y tener asociaciones internacionales constituyen una de nuestras grandes prioridades

Entrevistada por Karla Monterrosa-Yancey, CAMS, jefa de redacción, ACAMS, Miami, FL, EE. UU. editor@acams.org

PATRIOT OFFICER®

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

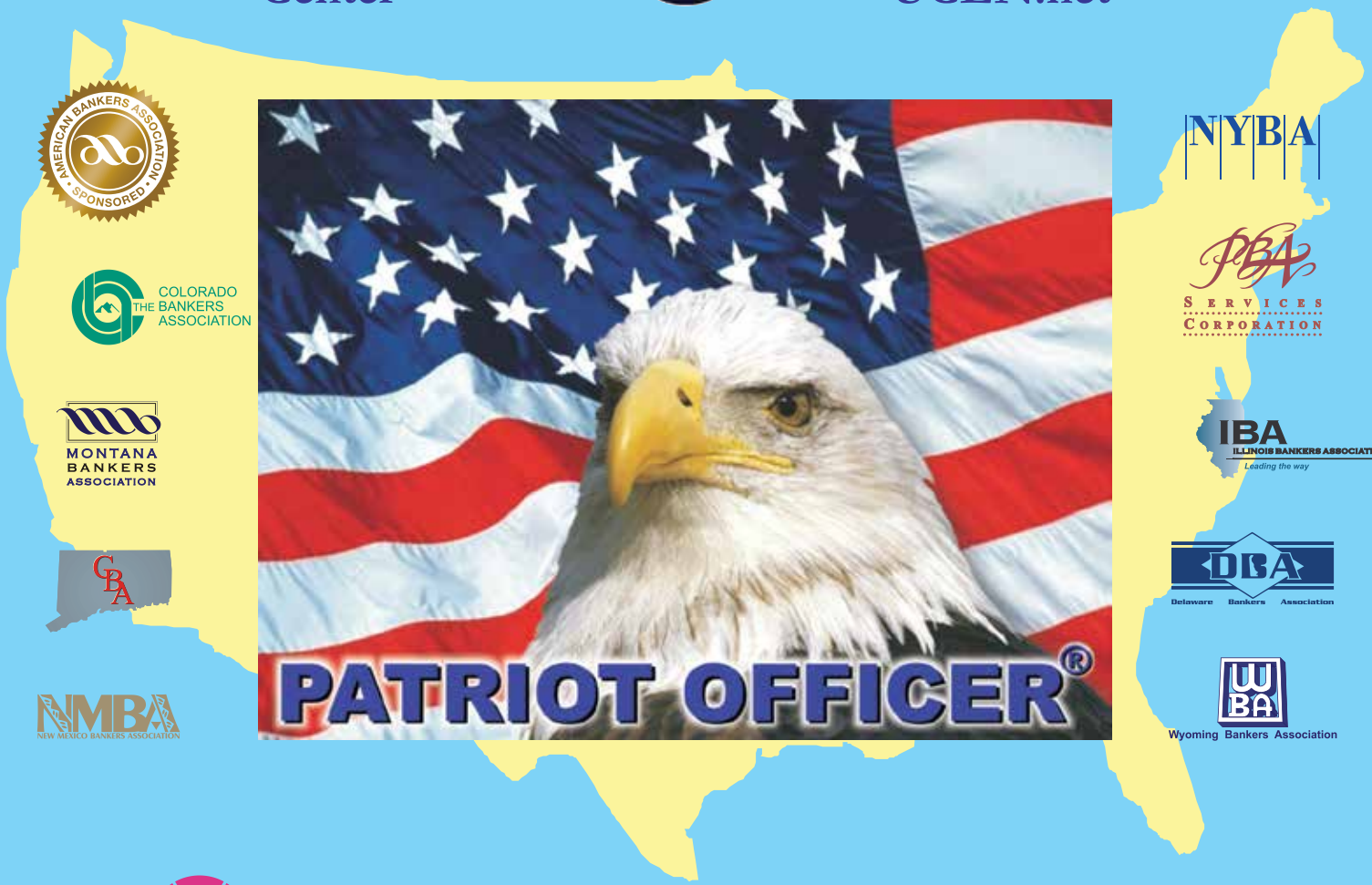
Endorsed By The Largest Bankers Associations and Has Passed Examinations

"THOUSANDS OF TIMES"

Financial Intelligence Center

UCEN

Compliance Network UCEN.net



GlobalVision Systems, Inc.

9401 Oakdale Avenue, Chatsworth, CA 91311

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

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

Ataque de los sintéticos

Desde el punto de vista de una entidad que debe informar sobre actividades sospechosas o delitos, tanto el intento de frenar la delincuencia como la aplicación de las leyes contra el financiamiento del terrorismo equivalen a implementar procesos de detección de nombres que coincidan en diferentes listas sensibles. Los nombres pueden provenir de fuentes abiertas (medios de información periodística), de departamentos gubernamentales como la OFAC (Oficina de Control de los Activos Extranjeros, por sus siglas en inglés), de otros organismos encargados de hacer cumplir la ley, o de varias listas confeccionadas por distintos gobiernos o entidades supranacionales (como las Naciones Unidas).

Los nombres sospechosos son comparados con la base de datos de clientes y en el caso de hallarse una coincidencia, se congelan los fondos de la persona o entidad en cuestión y se informa oportunamente a los organismos regulatorios apropiados.[1]

Los regímenes que regulan los informes o denuncias de financiamiento terrorista fueron diseñados alrededor de ese concepto central. El concepto ganó tal popularidad que se extendió a las sanciones y embargos con la denominación de "Sanciones Financieras Específicas".[2]

El principal supuesto implícito es que vincular un nombre con cierta información material (tal como fecha de nacimiento, número de seguridad social/número de seguro, número de pasaporte, etc.) conduce siempre a la identificación de un individuo. Sin embargo ¿qué pasa cuando un nombre vinculado a la información identificatoria es virtual o si el nombre es sintético (o sea que no existe)?

[1] Ver más en The Stockholm Process, en línea http://www.pcr.uu.se/research/smartsanctions/the_stockholm_process/ (Feb 19, 2013)

[2] Ver más en R. T. Naylor, Economic Warfare: Sanctions, Embargos Busting, and Their Human Cost (1999) Maple Press, York, Pennsylvania)

Este artículo cuestiona la premisa básica implícita en el régimen de denuncias del financiamiento terrorista mediante la identificación de una nueva tendencia muy preocupante: la identidad sintética.

No se trata de suplantación, ya que esto supone la existencia de una persona "X" que suplanta a otra persona "Y". Ambos individuos existen.

El escenario que estamos discutiendo es distinto. Aquí, ni "X" ni "Y" existen sino que son, en cambio, una creación virtual de otro "Z", que es en sí mismo una identidad virtual. Y todas esas identidades, al ser identificadas, dejan de "existir".

Es igualmente notable que cada una de estas identidades sintéticas están soportadas por documentación válida emitida por el gobierno de Canadá (por ejemplo, licencias de conducir y/o pasaportes, etc.).

Sin duda, se trata de un escenario escalofriante, algo parecido a lo que se lee en *Guerras Fantasma*, de Steve Coll, ya que apenas se detecta una identidad, ésta se desvanece en el aire, como si nunca hubiera existido. Lo único que queda son papeles que reflejan una cantidad exorbitante de ganancias obtenidas a través de delitos financieros que, por supuesto, son imposibles de rastrear (por ejemplo, en dos días alguien se adueñó de 710.000 dólares canadienses a través de fraudes de seguros, usando identidades sintéticas, y tanto los fondos como las identidades son imposibles de rastrear).

Este artículo está basado en la avanzada investigación que realizaron Michael Kelly y Timothy Trotter (Policía de Toronto), sin cuya permanente ayuda no habría sido posible escribirlo. Agradezco especialmente a Peter Warrack (Royal Bank of Canada) por su apoyo y su visión.

Acaso este artículo plantee más preguntas que respuestas. La primera parte detalla el proceso de creación de identidades, tal como hacen los delincuentes. La segunda, esboza cómo se cometen delitos usando identidades sintéticas. Y la última, señala las respuestas que hoy existen para combatir este delito formidable que, lamentablemente, son deficientes e ineficaces. Se alientan los debates futuros que exploren más opciones para combatir este nuevo tipo de delito.

Parte I

Una pregunta crucial aparece durante el estadio de creación de una identidad, en términos de los costos y riesgos que conlleva conseguir documentos emitidos por el gobierno: ¿por qué tomar un riesgo tan inmenso? Asumiendo que el enriquecimiento financiero sea el "único" propósito, lo mismo se puede lograr usando documentos fraudulentos. Entonces ¿por qué arriesgarse tanto para obtener documentos oficiales originales?

El proceso de creación de la identidad sintética

El sector privado — Génesis

Los pasos para crear una identidad sintética son, prima facie, preocupantemente simples. El delincuente suele comenzar por crear una silueta sin cara, usando un nombre, una fecha de nacimiento y un domicilio (por ejemplo, John Doe, fecha de nacimiento: 1 de enero de 1977, domicilio: Calle XY, provincia Z, Canadá).

Entonces, él o ella solicita una tarjeta de crédito en una entidad financiera importante, que normalmente busca una oficina de información crediticia para conocer la Declaración de Asuntos Personales (o sea, registros financieros, fecha de nacimiento, domicilio y calificación crediticia).

En este estadio no existe ningún registro, por lo que la respuesta suele ser negativa. Este rechazo es un paso clave en el proceso de creación de una identidad sintética porque obliga a la oficina de información crediticia a crear un registro con un nombre concreto, que a partir de ese momento queda vinculado con un domicilio y una fecha de nacimiento.

Es ese rechazo inicial de una tarjeta de crédito lo que sirve como génesis para las identidades sintéticas en el mundo de las finanzas: la información personal queda documentada en una oficina de información crediticia y pasa a ser "real" sin despertar ninguna alerta. Esto es así porque esas oficinas no pueden determinar si una persona existe o no, ni pueden diferenciar o examinar una identidad basándose con cómo o dónde emergió por primera vez. Desde la perspectiva de la entidad financiera, cualquier solicitud de tarjeta de crédito puede ser rechazada, por lo que es totalmente normal que una "persona nueva" sea rechazada.

Luego, los delincuentes solicitan una tarjeta de compra en alguna tienda minorista con un límite de crédito nominal para escapar al análisis minucioso. Estas tarjetas suelen requerir un documento a la vista que verifique el nombre, la fecha de nacimiento y el domicilio del solicitante. Para conseguir la tarjeta de compra, usan generalmente el documento de rechazo de la entidad financiera que detalla sus datos.

Una vez obtenida, la usan para mejorar la calificación crediticia haciendo compras y pagos regulares. Al tiempo, solicitan tarjetas adicionales, que suelen obtener sin problema. Éstas se usan de modo similar.

El tiempo es aliado del delincuente: cuanto más tiempo se use una tarjeta de compra o de crédito sin generar problemas, más inexpugnable se vuelve la identidad sintética. La actitud que prevalece suele ser: "John Doe ha sido un cliente bueno y leal durante dos años", y así se va afianzando la identidad.

Resumiendo: inicialmente se explota el sector privado de manera sistemática para construir una identidad sintética. Cuando ésta está adecuadamente madura, se la empieza a usar para acceder al sector público.

Sin embargo, si el enriquecimiento financiero fuera el "único" propósito, éste podría considerarse ahora cumplido. Por lo tanto, los próximos pasos (teniendo en cuenta este propósito asumido) podrían parecer innecesarios, en principio.

El "Rostro"

Una persona real que pueda ser fotografiada es vital, si no indispensable, para la mayoría de los documentos del sector público. Los delincuentes suelen usar rostros de personas que no tienen nada que ver con ellos para conseguir documentos del sector público. A veces, esas personas son visitantes de alguna otra jurisdicción o provincia, y otras, son empleados con salarios bajos a los que se promete un trabajo mejor o sustanciales sumas de dinero por tareas menores (como acompañar a alguien a abrir una cuenta bancaria).

Hubo un conocido caso en el que se usó el rostro del hijo de un diplomático indio, empleado en un café por un salario bajo. El delincuente (en este caso, el "Controlador") visitó el café, inició una conversación con el hijo del diplomático, quien le dijo que estaba buscando un trabajo mejor pago. No hace falta decir que fue contratado.

Los investigadores consideran a estas personas víctimas y las llaman "Rostros" porque los datos (nombre, domicilio, fecha de nacimiento, número de seguridad social, etc.) asociados con ellas son falsos, y lo único verdadero es su rostro.

Un Rostro cumple un rol esencial en este ciclo de crimen porque él o ella facilita la apertura de cuentas bancarias *en persona*, la firma de contratos financieros *en persona*, la firma de contratos de alquiler *en persona*. Los delincuentes pueden hacer todo lo demás a distancia.

O sea, los delincuentes se distancian de sus crímenes usando un Rostro, que queda asociado con una actividad criminal que no les pertenece.

El sector público

El sector público permite acceso a través de sobornos y corrupción o usando documentos del sector privado y/o documentos (legítimos o fraudulentos) expedidos por el gobierno (extranjero o doméstico).

Corrupción

Hubo un caso en que dos empleados del Departamento de Tránsito — encargado de expedir licencias de conducir — aceptaron aproximadamente 250 dólares canadienses por licencia para procesar y expedir múltiples licencias para uno o varios Rostros. Por ejemplo, un Rostro obtuvo 13 licencias de conducir (usando 13 nombres y domicilios distintos) en el mismo lugar.

Los investigadores examinaron trescientas licencias expedidas por los dos empleados durante un año y encontraron que cerca de doscientas eran fraudulentas. A medida que la investigación se amplió, se identificaron varios empleados de otras oficinas otorgadoras de licencias que emitían múltiples licencias para varios Rostros.

Otra documentación usada para para obtener licencias de conducir

El sitio web del Departamento de Tránsito de Ontario explica que para obtener una licencia de conducir de esa provincia, el solicitante deberá "mostrar pruebas de su nombre legal, fecha de nacimiento (debe incluir el día, el mes y el año de nacimiento) y firma del interesado. Los documentos deben ser originales y válidos".[3]

La prueba principal que usan los delincuentes para solicitar licencias de conducir son las tarjetas de compra, las tarjetas de crédito y las cartas de rechazo de las entidades financieras. Si les exigen otros documentos para apoyar la solicitud, usan Tarjetas de Ciudadanía Canadiense, documentos que acrediten condición de refugiados y pasaportes extranjeros, auténticos o falsos.

Dichos documentos son inherentemente problemáticos porque, a pesar del entrenamiento, es difícil diferenciar los documentos auténticos de los fraudulentos. También sucede que los documentos de los ciudadanos canadienses de más edad carecen de elementos de seguridad, lo que hace imposible verificar su autenticidad.

Los pasaportes extranjeros (falsos o genuinos) que se usan como documentos de apoyo también son problemáticos, debido al entrenamiento insuficiente, a la falta de recursos, a los procesos anticuados y a las limitaciones de tiempo de los empleados.

Los delincuentes también solicitan pasaportes canadienses usando diferentes Rostros. En algunos casos, usan documentos que acreditan status de Refugiados (intrínsecamente complicados por la poca documentación requerida para este proceso) y, en otros casos, hacen una denuncia policial por "pasaporte robado", que se usa entonces para hacer una nueva solicitud de pasaporte canadiense.

Números de Seguro Social

A veces, para reforzar aún más una identidad, se usa un Número de Seguro Social Canadiense (SIN, por sus siglas en inglés, equivalente al Número de Seguridad Social de los EE. UU.). Sin embargo, no hace falta un SIN para conseguir una tarjeta de crédito, para abrir una cuenta bancaria o realizar ciertas transacciones (como hipotecas, líneas de crédito, préstamos), para solicitar una licencia de conducir, alquilar un auto o, incluso, ofrecer un contrato de alquiler.[4]

Los SIN son necesarios para tratar con el gobierno (por ejemplo, para presentar la declaración de impuestos y para obtener servicios médicos y sociales). Las entidades financieras y las compañías de seguros también pueden pedir el SIN para sus registros[5] o para realizar ciertas operaciones complejas.

Pero la cuestión es que los SIN han sido usados por los delincuentes para hacer transacciones financieras. Asumiendo que el enriquecimiento financiero es el "único" propósito del delito, cabe hacerse la siguiente pregunta: ¿por qué conseguir documentos expedidos por el gobierno si es que no son necesarios?

Probablemente se lo haga para dar una apariencia de autenticidad adicional a la actividad delictiva o porque la identidad sintética acaso tenga otras ventajas, además de la "mera" ganancia financiera ilícita.

Una intrincada red de identidades

Usando estos métodos, los delincuentes crean múltiples identidades sintéticas, que, a su vez, sirven de apoyo para otras nuevas. La mayoría de ellas tiene documentos emitidos por el gobierno y calificaciones crediticias impecables.

Durante un caso, cuando los investigadores trabajaban con los sectores público y privado para analizar datos asociados con un puñado de datos identificatorios (nombres, domicilios, números de teléfono, etc.), el número de identidades sintéticas creció hasta aproximadamente 1.000. Por ejemplo, cuando los investigadores buscaron un número de teléfono asociado con el nombre de una identidad sintética, descubrieron que el mismo número de teléfono había sido usado para activar tarjetas de crédito para otras 50. Este intrincado proceso en red siguió regenerándose *ad infinitum*.

Parte II

Delitos que se cometen usando identidades sintéticas

Generación de ingresos

Una vez creada, la identidad sintética se utiliza para diversos propósitos ilegales. Los dos principales son la generación de ingresos y la logística. Si bien esta división no es rígida y los usos suelen superponerse, el primer propósito se desarrolla minuciosamente durante períodos prolongados, generalmente de dos a tres años. La generación de ingresos se trabaja con el mayor cuidado — hasta que es "reventada" — las calificaciones crediticias se optimizan concienzudamente con los pagos a tiempo y los puntajes de crédito se mejoran de manera lenta pero segura.

Una vez que las calificaciones crediticias han mejorado sustancialmente y que la identidad ha madurado lo suficiente, se las aprovecha para adquirir bienes de alto valor (como productos de seguros, etc.) que generan una tremenda cantidad de ganancias antes de ser "reventadas" y descartadas.

Normalmente, en los "revientes" los delitos financieros se cometen de una manera sincronizada y sistemática durante una duración muy corta. Esto puede incluir tarjetas de crédito robadas, cuentas bancarias vaciadas, fondos transferidos internacionalmente, adelantos de efectivo máximos, sobres vacíos depositados en los cajeros automáticos, seguidos por retiros de efectivo, y compra de pasajes aéreos de ida.

Los "revientes" tienen el potencial de recaudar un monto significativo. Por ejemplo, una sola identidad sintética puede juntar decenas de miles de dólares en pocas horas. Una estafa prolongada (dos días) que involucre varias identidades puede recaudar millones de dólares.[6]

[3] Sitio web de Ontario Motor Vehicles: http://www.mto.gov.on.ca/english/dandv/

[4] Service Canada en línea: http://www.servicecanada.gc.ca/eng/sin/info/yoursin.shtml

[5] Las entidades financieras y otras empresas que deben informar de sus transacciones no usan información personal o números SIN cuando envían informes al FINTRAC (Centro de Análisis de Informes y Transacciones Financieras de Canadá, por sus siglas en inglés) o a la OSFI (Oficina del Superintendente de Entidades Financieras de Canadá).

[6] Ver más en: United States District Court, District of New Jersey, United States of America vs. Babar Qureshi et al. Criminal Complaint No. 13-8013 (MAC)

Uso logístico

Las identidades sintéticas también se usan fuera del ámbito del "mero" delito financiero. Por ejemplo, a veces se instalan refugios anónimos (o sea, departamentos que, alquilados bajo una identidad sintética, son convertidos en escondites para varios individuos), se compran o alquilan camiones u otros vehículos pesados y se compran planes de teléfonos celulares a nombre de alguna identidad sintética.

También se han facilitado viajes internacionales con relativa impunidad usando identidades sintéticas. Hubo un caso en que Interpol se contactó con investigadores para pedir más información respecto de una persona en custodia cuyos documentos de viaje reflejaban un nombre que había sido marcado como de identidad sintética por la policía de Toronto. Se alertó a Interpol que el individuo no era la persona descripta en los documentos. Los documentos creaban una identidad sintética. Sin embargo, tome nota: es muy posible que las búsquedas basadas en documentos de viaje y otros documentos accesorios no revelen ningún registro criminal o policial.

Logística y generación de ingresos

La división entre esos dos usos a menudo se desdibuja. Tomemos por ejemplo la inscripción en línea de una compañía de construcción y de transporte en camiones. La tarjeta de crédito que se use será "válida" *per se* (o sea, expedida por una entidad financiera que pertenece a una identidad sintética). El domicilio registrado también será "válido" *per se* (una ubicación existente se alquila a una identidad sintética) y los directores, accionistas y empleado serán individuos aparentemente reales (pero que son todos identidades sintéticas). En tales circunstancias, no sólo se desdibuja la división sino que también se hace más problemática. No es probable que la compañía atraiga atención si compra camiones o transporta bienes restringidos.

En un caso, una identidad sintética "compró" un camión de 21 metros, que pesaba 36 toneladas. El dueño registrado era una identidad sintética y el conductor también. La mercadería se exportaba a África ya que toda la documentación requerida había sido considerada como "apropiada".

En otro caso, una compañía registrada por una identidad sintética compró y contrató un seguro completo en Alberta. Los camiones fueron puestos en vagones de ferrocarril y transportados a la costa Pacífico, desde donde se los envió a Dubai. Posteriormente, fueron denunciados como robados y se reclamó el seguro. Asumiendo que los camiones fueron vendidos (cuestan aproximadamente 300.000 dólares cada uno) y que se cobró la totalidad del seguro, la ganancia neta sería del 150 por ciento del precio de compra (900.000 dólares), menos unos pocos meses de pagos al seguro antes de ser denunciados como "robados".

Bienes restringidos

También es alarmante con qué facilidad se pueden obtener bienes y commodities restringidos usando identidades sintéticas.

En muchas jurisdicciones, la compra de productos químicos, industriales o restringidos supone un proceso que requiere presentar una identificación antes de la compra. Cuando se alcanza una cantidad predeterminada, establecida como referencia, se hace obligatoria una presentación. Este requisito obliga al vendedor a informar sobre la venta a las autoridades correspondientes y a presentar ciertos detalles (por ejemplo, que una cierta compañía o persona ha comprado la cantidad umbral de un producto químico o industrial durante el período referido en el informe). Sin embargo, si diez personas "distintas" compran productos restringidos durante el período aplicable, no es probable que las operaciones se noten, porque no aparecerá el mismo nombre más de una vez (aunque las diez identidades sintéticas pertenezcan a la misma persona). El nivel umbral no se alcanza y, por lo tanto, no hay alertas. Cada uno de estos ejemplos debería encender muchas luces rojas de alerta, exigiendo atención inmediata y extraordinaria, pero actualmente esto no ocurre.

Parte III

Respuestas para combatir la identidad sintética

¿Cómo se está combatiendo este delito formidable?

Lamentablemente, la respuesta para combatir este delito es profundamente deficiente. Hay varias razones para eso.

Por lo pronto, la identidad sintética es una tendencia criminal nueva, que todavía debe ser comprendida por la mayoría y/o ganarse un lugar en los códigos penales de las distintas jurisdicciones. Por lo tanto, la respuesta a este delito quedó retrasada, en el sentido de que para combatirlo se usan recursos y destrezas ya existentes. Ésta es una limitación aguda. Los departamentos gubernamentales están orientados a combatir los delitos tradicionales ya existentes, la mayoría de los cuales ni se acerca, en términos de potencial y gravedad, a este nuevo género de delito.

Los departamentos trabajan en silos aislados

Los departamentos gubernamentales están inherentemente limitados y restringidos, ya que trabajan en silos aislados. Aquéllos que podrían hacer frente a semejante delito — ya sea la policía, la inteligencia, la seguridad nacional, etc. — sufren penosas barreras burocráticas restrictivas y otras limitaciones que dificultan el intercambio de información en tiempo real. Lejos de ser sólo una opción, la integración es un imperativo y una necesidad.

La integración y el intercambio de información en tiempo real fue una recomendación clave de la Comisión 9/11 de los Estados Unidos. Sin embargo, la mayoría de las naciones aún tiene que tomar conocimiento de ella. Muchos países están agobiados por engorrosas barreras al intercambio de información. En muchos casos, los departamentos de policía, inmigración, seguridad social y tránsito vehicular enfrentan barreras burocráticas y preocupaciones sobre la privacidad que impiden, cuando no prohíben, el intercambio de información en tiempo real.

Los silos claramente benefician a los delincuentes. Idealmente, la Oficina de Pasaportes de Canadá debería tener acceso a los mismos datos que Control de Fronteras, Inmigración y otros departamentos relevantes. El intercambio de información en tiempo real tiene un inmenso valor.

Por ejemplo, si una identidad sintética llamada John Doe solicita una licencia de conducir, el Departamento de Tránsito (a través del Ministerio de Transporte) podría asegurarse de que el pasaporte canadiense o el documento de status de refugiado coincida con los datos de que disponen los servicios de inmigración.

Los distintos departamentos deberían estar integrados y empoderados para intercambiar información en tiempo real o tener la capacidad de acceder a la misma.

Controles centrados en los puntos de entrada

Nuestro sistema de seguridad ha creado controles que están centrados en los puntos de entrada. Asumiendo que alguien compromete o viola la seguridad en uno de ellos, todo el sistema queda comprometido y el delincuente obtiene acceso irrestricto a todo el sistema. Una vez que entró, es virtualmente imposible distinguir a un delincuente de un usuario legítimo. Tampoco se pueden evitar sus acciones. En ese sentido, el incidente de soborno en el Departamento de Tránsito es bien indicativo.

Cuando se violaron los controles en el Departamento de Tránsito y se obtuvo la licencia de conducir, se consiguió acceso libre para conseguir crédito y construir calificaciones crediticias estelares, abrir múltiples cuentas bancarias, conducir transacciones financieras complejas, contratar seguros, alquilar vehículos pesados, comprar bienes restringidos y firmar contratos de locación sin despertar ninguna alerta.

Modernizando los Sistemas

La tecnología usada por muchos departamentos de gobierno es inadecuada para hacer frente a este nuevo delito. Por su lado, los delincuentes usan tecnología sofisticada y tienen conocimiento sobre las limitaciones tecnológicas.

Tomemos, por ejemplo, la Tecnología de Comparación de Fotos (TCF), usada por el Ministerio de Transporte y por Pasaportes de Canadá. Está construida sobre una lógica defectuosa. Los funcionarios del gobierno creen que si se utiliza correctamente la TCF, ésta proporcionará información adecuada en el momento oportuno. Depende de que un Rostro o un iris exista múltiples veces en la misma base de datos para que sea marcado. Entonces, si el Rostro o el iris no aparece en la base de datos, no será considerado fraudulento.

En los casos de identidad sintética, se usan muchos Rostros. Los Rostros, como dijimos, suelen ser visitantes de otra provincia o jurisdicción, de modo que no existen registros de esas personas. Cuando se usa un nuevo Rostro, la TCF es sobrepasada y derrotada. O también, el sistema puede ser engañado si hay un ligero cambio en el ángulo en que la persona mantiene su cabeza o si cruza un poco los ojos.

Incluso si se moderniza la tecnología TCF, es debatible su eficacia real porque no podrá *per se* impedir la creación de una identidad sintética. Pero la tecnología TCF puede limitar a los delincuentes ya que no podrán usar un Rostro para crear múltiples identidades (sólo un nuevo Rostro/par de ojos por identidad). Sin embargo, no podrá impedir que los delincuentes creen de la nada una identidad sintética que el sistema no detectará porque el Rostro/los ojos aparecen una sola vez bajo ese nombre.

Una vez dicho esto, hay que tomar conciencia de que la tecnología es una herramienta, esencial, pero herramienta al fin y no está ipso facto a la par de la inteligencia, habilidad o capacidad humanas. Además, la tecnología puede llevar a la complacencia si sus limitaciones inherentes no son comprendidas a priori. Para responder a este delito de modo eficaz, es imprescindible un cambio de mentalidad. La clave está en la agilidad y en el pensamiento creativo, más allá de la comodidad y de los procesos tecnológicos estándar.

Otros puntos vulnerables

Existen muchos puntos vulnerables que exigen atención. Por ejemplo, habría que revisar la categoría y el proceso de status de Refugiado para evitar su mal uso.

Las Tarjetas de Ciudadanía Canadiense expedidas décadas atrás eran tarjetas laminadas, sin elementos de seguridad. Muchas de ellas se encuentran todavía en circulación y se usan para completar la documentación adicional requerida para obtener una licencia de conducir o abrir una cuenta bancaria. Deberían cancelarse y discontinuarse inmediatamente.

El Departamento de Inmigración de Canadá debería emprender un estudio exhaustivo de otros procesos jurisdiccionales. Por ejemplo, algunas jurisdicciones incluyen tarjetas biométricas en los documentos de identificación (pasaportes, licencias, etc.). Habría que estudiar más esas opciones.

Tomemos otro ejemplo: el Centro de Análisis de Informes de Transacciones Financieras de Canadá tiene prohibido aceptar números SIN debido a cuestiones de privacidad y otras preocupaciones. Estos datos clave podrían hacer más eficientes las investigaciones.

Conclusión

La identidad sintética es una tendencia nueva y extremadamente significativa que ha cambiado las nociones tradicionales sobre los delitos financieros.

Las espectaculares y extensivas leyes de financiamiento terrorista promulgadas después del 11/9 fueron inmediatamente seguidas por una ola de regulaciones y pautas que detallaban la conducta esperable de la mayoría los actores comerciales de nuestra sociedad. Un componente central de esas leyes exigía que las entidades que deben enviar informes cuenten con procesos integrales que busquen, detecten y congelen los fondos de un cliente si se sospecha alguna actividad sospechosa. Este proceso, a pesar de su limitación, funcionó bien durante una década.

Sin embargo, la identidad sintética ha cambiado el juego. Los conceptos convencionales que propulsaron esas leyes ahora son mayormente inaplicables. Esto es porque las identidades sintéticas se crean de la nada, tienen la capacidad de recaudar cantidades significativas de fondos, y, cuando son identificadas, tienen la capacidad de desaparecer sin dejar rastro. La proscripción, la búsqueda, la detección y el congelamiento de activos son de poca ayuda para combatir un delito tan serio.

Esta tendencia es también muy significativa porque la creación de identidades sintéticas es un emprendimiento inmenso logístico

Esta tendencia es también muy significativa porque la creación de identidades sintéticas es un emprendimiento inmenso logístico. No es una tarea ad hoc perpetrada una sola vez por un grupo de individuos desesperados o sin guía. Sin ninguna duda, es un modus operandi metódico puesto en práctica por un grupo criminal bien disciplinado, organizado y financieramente sofisticado. Por un lado, este grupo tiene la capacidad para controlar recursos logísticos importantes bajo la cubierta del anonimato y, por el otro, genera un inmenso flujo de ingresos cuando el aspecto logístico se hace innecesario.

Y, lo que es igualmente alarmante, este delito no tiene precedente y no existen características o tendencias en este contexto. En otros casos de delitos graves, existieron similitudes o tendencias distinguibles. Sin embargo, en este caso, las personas (esto es, los "Rostros", sus "Controladores" y/o delincuentes) no tienen nada en común. No comparten una ideología, religión, cultura, idioma, nacionalidad u origen.

No existen factores comunes, patrones o tendencias entre los Rostros y sus Controladores. Provienen de distintos países, hablan innumerables idiomas y no comparten una cultura o una religión, más allá de que son todos adultos y que la mayoría de los Rostros están en una situación financiera desesperada.

En conclusión, este artículo claramente plantea más preguntas que respuestas. Esto es así porque mi intención no es la de aportar un análisis exhaustivo del delito, su metodología o, ni siquiera, las acciones de respuesta. Lo que deseo, en cambio, es llamar la atención sobre esta nueva tendencia y generar un debate sobre cómo combatirla.

Dr. Kalyani Munshani, senior manager, Global AML Compliance, Royal Bank of Canada, Toronto, Canada, Kalyanimunshani@gmail.com

Las ideas y opiniones expresadas en este artículo pertenecen exclusivamente al autor y no representan al Royal Bank of Canada o sus filiales.

acamsglobal.org

ACAMS 12th Annual

AML & Financial Crime CONFERENCE

PRE-CONFERENCE TRAINING: SEPTEMBER 22, 2013
MAIN CONFERENCE: SEPTEMBER 23–25, 2013

ARIA ■ LAS VEGAS

The industry's most influential and comprehensive training conference puts financial crime front and center

Featuring 9 targeted learning tracks including NEW focus on Risk Management, AML Core Training and Non-Depository Institutions; plus expanded Audit Workshops

The latest regulatory developments and practical guidance for clearer understanding of the impacts on your institution

Peer-to-peer information sharing across 55+ interactive sessions, networking events and the first-time AML Think Tank, where YOU decide the topics for discussion

Early bird discount through June 28

SAVE $300

Register today with VIP code PT-300
acamsglobal.org | +1 305.373.0020 | info@acams.org

*Register and pay by June 28, 2013 with VIP code PT-300 and save $300 off the standard, non-government main conference price. Pre-conference workshops and the CAMS Exam Prep Seminar are not included in main conference pricing. Additional discounts are available for government, law enforcement and groups of 3 or more. Please contact Geoffrey Fone at gfone@acams.org or at +1 786.871.3021 for details. Discounts cannot be combined .

El Monte de Tres Barajas en el Antilavado de Dinero

Ilustración por John Nicoll

En este viejo juego de embaucadores, se mezclan tres cartas delante de tus ojos con la promesa de un pago si eres capaz de elegir tu carta después de que el timador haya barajado el conjunto de una manera aparentemente inocua. Muchos pierden unos cuantos dólares antes de darse cuenta de que fueron vencidos por las distracciones mentales y verbales que indujo el embustero y no por una particular forma de barajar. En las acciones Antilavado de Dinero (ALD) suele ocurrir un fenómeno similar, cuando el investigador se distrae con los movimientos del dinero antes de darse cuenta de que se le escapó el mecanismo real de lavado.

Casi todas las estafas y fraudes exitosos se basan en reacciones emocionales y distracciones que prevalecen sobre un prudente escrutinio financiero. Después de todo, el lavado de dinero es una estafa que no tiene una víctima manifiesta. Los lavadores de dinero exitosos aprendieron a crear y explotar las distracciones emocionales y de otro tipo. La compra, el propósito o el gasto reales (integración) serán razonablemente explicables siempre y cuando tu investigación pueda ser desviada del trabajo hormiga de colocación y estratificación que se ocupó de poner allí el dinero.

La mayor parte de las transacciones legítimas se hacen de una manera lo más lineal posible para cumplir un propósito determinado. Por ejemplo, los dineros ahorrados pueden ser transferidos a una cuenta corriente para hacer un pago mayor de lo habitual, como ocurre al comprar un auto. No serviría a ningún propósito legítimo transferir el dinero a través de otras cuentas u otras personas antes de colocarlo finalmente en la cuenta corriente que se usará para comprar el auto con un cheque. En lavado de dinero, esos movimientos extra son comunes y se hacen deliberadamente para provocar distracciones respecto de la fuente real y del beneficiario del dinero implicado. Muchas veces el subterfugio está tan estratificado como las transacciones y nunca refleja la naturaleza deliberada del plan general.

Podrás pensar que tu investigación te condujo a esa flamante adquisición de un auto nuevo que descubriste, cuando, en realidad, el dinero lavado ya se dispersó varias transacciones atrás. El dueño del nuevo auto estará bien desconectado de esos hechos. Como en el caso de la baraja equivocada, te concentraste en el reo equivocado.

Muchos de esos esquemas involucran segundas y terceras personas y pueden también incluir compradores nominales o testaferros en el camino. Si bien muchos de los que participan están al tanto de la situación, el agregado de un participante o estrato involuntario agregará elementos emocionales, distracciones y complicaciones que pueden desinflar y descarrilar el entusiasmo de cualquier investigador por continuar su tarea. Aunque esas distracciones parecen inocuas, son deliberadas y están bien planeadas, justamente para lograr ese efecto.

Por ejemplo, la cuenta de una empresa refleja repentinamente un sospechoso flujo de depósitos en efectivo. Cuando se contacta al propietario, éste confiesa que está escondiendo dinero para un amigo muy cercano, que está atravesando un divorcio difícil. Se retrata a sí mismo como un hombre honesto en otros aspectos pero con el gran defecto de estar siempre dispuesto a ayudar a un amigo en problemas. También pinta una compasiva historia de su amigo que está siendo muy maltratado durante su divorcio y reconoce que se le hizo muy difícil no querer ayudarlo, dadas las dolorosas circunstancias.

Este barajar de beneficiarios hace que la reorientación de la investigación se complique desde los puntos de vista mental y logístico. A quién vas a investigar y por qué motivo se convierte en un problema. La perspectiva de meterte en un desagradable divorcio se suma como una nueva e incómoda razón para que no quieras continuar.

A efectos de nuestra argumentación, digamos que das el próximo paso y te contactas con ese desdichado beneficiario. Su historia coincide con la de su amigo y refuerza los detalles desagradables del divorcio. Se culpa a sí mismo por poner a su amigo en semejante apuro y se lamenta de todos los problemas que esta situación ha infligido en su vida. También te expresa con emoción que su vida va a quedar totalmente arruinada porque posiblemente su vengativa ex se va a enterar de todo esto. "Caso perdido" describe bien la impresión que te deja el pobre hombre.

Como investigador, te dices que tu trabajo es el de encontrar auténticos casos de lavado y no el de involucrarte en un divorcio escabroso. En este punto, todo lo que quieres hacer es encontrar algún tipo de forma aceptable para cerrar el caso.

En lo que fue el caso real esbozado arriba, un amigo de la esposa se presentó a informar que el divorcio se debió a que ella estaba harta de un esposo que se dedicaba a consumir y vender drogas. El colmo fue cuando lo encontró en casa con su bebé en las rodillas mientras cortaba la cocaína para vender. Esta esposa no quiere denunciarlo por miedo a perder la pensión alimenticia y la manutención de sus hijos. Bingo, finalmente se dio vuelta la carta correcta.

Las emociones y el dinero van de la mano. En antilavado tienes que aprender a reconocer la emoción e investigar su propósito, tanto como el propósito del dinero. Un buen investigador siempre considerará y tratará las respuestas cargadas de emoción como prueba potencial, en vez de dejarse distraer por ellas. Los talladores de este juego — los estafadores y los lavadores de dinero — sólo pueden triunfar aprovechando las distracciones que provocan. Crean y luego explotan las emociones. Resulta siempre prudente que te preguntes si algún bloqueo emocional te está impidiendo ver algo evidente.

En el mundo de las actividades legítimas — especialmente en el caso de compras grandes como automóviles e inmuebles — la creación o la explotación de un entorno emocional son consideradas buena táctica de ventas. Los vendedores de autos insertan docenas de agregados que, muchas veces, suman ganancias. El comprador suele estar demasiado atrapado por el brillante auto nuevo como para siquiera darse cuenta. Hay muchas similitudes con las relaciones ilegítimas emoción/dinero que se pueden identificar en esas tácticas.

Casi siempre que se atrapa un canalla lavador de dinero sus asociados denunciarán sospechas que no se habían "animado" a presentar. Las más de las veces, temían mancillar una reputación estelar que el reo había impulsado. Tómate tu tiempo para examinar cómo se crean y mantienen esos entornos emocionales y así empezarás a reconocerlos mejor, sin dejarte distraer por ellos. Toma nota, y no apego, de las emociones. Sé un espectador del Monte de Tres Barajas, nunca un jugador. A

Steve Gurdak, CAMS, supervisor, Washington Baltimore HIDTA, Northern Virginia Financial Initiative (NVFI) Annandale, VA, USA, sgurdak@wb.hidta.org

ACAMSToday.org is now mobile!

www2.acams.org/TheApp

ACAMS members may now download the *ACAMS Today* App and read relevant articles and content directly from their mobile devices.

Download the App for:

- **Full access to the complete compendium of articles, interviews, polls and exclusive content available to ACAMS members**
- **An easy-to-use interface that allows you to find the information important to you**
- **Convenient access to content wherever and whenever you want**

Get the app now at

www2.acams.org/TheApp

El papel de los reguladores en la supervisión de la Ley de Secreto Bancario y de Antilavado de Dinero

Este artículo está basado en una revisión de las declaraciones que Thomas J. Curry, titular de la Oficina del Controlador de la Moneda (OCC — Office of the Comptroller of the Currency) — dependiente del Departamento del Tesoro de los Unidos — efectuó ante el Comité de Banca, Vivienda y Asuntos Urbanos del Senado de EE. UU. el 7 de marzo de 2013. En sus declaraciones, Curry ofrece una visión de los criterios de supervisión y de las prácticas de cumplimiento que usarán los inspectores de dicha Oficina en sus permanentes esfuerzos para supervisar a los Bancos Nacionales y Asociaciones Federales de Ahorro (bancos), respecto de la Ley de Secreto Bancario (LSB) y de cumplimiento Antilavado de Dinero (ALD).

El Controlador Curry hace hincapié en que los inspectores deben aplicar acciones enérgicas y proporcionar procedimientos de supervisión rigurosos para asegurar el cumplimiento de las leyes; pero también en que deben trabajar con los banqueros, escuchar las preocupaciones de la industria y trabajar continuamente para mejorar el proceso de supervisión LSB/ALD.

Observaciones e información general

El Controlador Curry comenzó su testimonio presentando los antecedentes de las leyes LSB/ALD. Hizo varias observaciones y reconoció varios problemas que afectan el cumplimiento LSB/ALD. Dichas observaciones incluían:

- Las metas de la OCC son las de disuadir el lavado de dinero, la financiación del terrorismo y otras actividades delictivas que se pueden ejercer a través de las instituciones financieras de la nación.
- La OCC está comprometida a asegurar que las entidades financieras bajo su supervisión tengan controles eficaces que las protejan de ser usadas para lavar dinero, financiar el terrorismo o facilitar la actividad criminal.
- Los bancos están obligados a denunciar las actividades sospechosas desde la década del 70 y, a tener un programa de cumplimiento LSB/ALD, desde 1987.
- Desde los 70 y los 80, los requerimientos regulatorios y las expectativas de supervisión para LSB/ALD han aumentado, y muchos bancos se vieron obligados a mejorar sustancialmente sus programas LSB/ALD.
- La mayoría de los 5,6 millones de SAR (Informes de Actividades Sospechosas, por sus siglas en inglés) ingresados en la base de datos de la FinCEN (Red de Cumplimiento de las Leyes de Delitos Financieros, por sus siglas en inglés) fue presentada por bancos supervisados por la OCC.
- El cumplimiento de las leyes LSB/ALD es difícil, porque los bancos tienen que revisar un gran volumen de transacciones para poder identificar las actividades sospechosas.
- La sofisticación y la determinación de los lavadores de dinero, terroristas y delincuentes ha aumentado significativamente en los últimos años.
- Los delincuentes pueden usar (y usan) la tecnología, los productos y los servicios ofrecidos por los bancos para mover dinero instantánea y anónimamente alrededor del mundo.
- Los sistemas de lavado se están haciendo cada vez más complejos y más internacionales.
- Los bancos se vieron obligados a dedicar mayor cantidad de recursos para mantener programas LSB/ALD eficaces.
- Los reguladores han tenido que aumentar significativamente su actividad de supervisión de LSB/ALD.

Tendencias y preocupaciones

El Controlador Curry declaró que muchos problemas de cumplimiento LSB/ALD que los bancos tuvieron en el pasado fueron debidos a debilidades en cuatro áreas principales:

- La cultura de cumplimiento de la organización
- La asignación de recursos expertos y suficientes.
- La fortaleza de la tecnología informática y del proceso de monitoreo de cuentas.
- Las prácticas de gestión del riesgo.

Declaró a continuación que los problemas en estas cuatro áreas generaron debilidades en los principios básicos LSB/ALD y señaló un número de preocupaciones respecto de los programas LSB/ALD. Aparecen debilidades en las siguientes áreas:

Gerencia — Las recientes inquietudes de supervisión mostraron que algunos bancos tienen una filosofía de gobernancia corporativa débil, que resulta en una "cultura de cumplimiento" pobre. La dirección no hace hincapié en la importancia del cumplimiento LSB/ALD, la función de cumplimiento no tiene independencia, suele tener más importancia el crecimiento y la generación de utilidades

que la preocupación por una gestión de riesgos adecuada, y no se asume responsabilidad por la función LSB/ALD. En resumen, la dirección no inculca las ideas de que el cumplimiento LSB/ALD es importante y de que va a asegurar que se cumplan las leyes y regulaciones LSB/ALD.

Recursos — Muchas debilidades demostraron ser resultado directo de la falta de suficiente personal capacitado, de una alta tasa de recambio de personal, y de recortes de gastos que provocan incumplimiento. Las inspecciones LSB/ALD encontraron también que, debido a la crisis financiera, varios bancos recortaron el personal de LSB/ALD, sin aumentarlo después cuando el banco creció o cuando desarrolló nuevos productos y servicios.

Productos y Servicios — Los bancos ampliaron el uso de servicios y productos de mayor riesgo sin desarrollar estrategias apropiadas para la gestión del riesgo. Esos servicios y productos incluyen: banca correspondiente extranjera, transferencia de fondos en el exterior, grandes repatriaciones de efectivo, captura de depósitos remotos y servicios bancarios para embajadas.

Riesgos para los bancos más pequeños — Algunos bancos grandes y medianos tomaron medidas para disminuir su exposición a los riesgos, reduciendo la exposición a clientes de mayor riesgo y la cantidad de productos y servicios riesgosos. Los bancos más pequeños, que a veces no tienen el personal o los conocimientos suficientes para gestionar adecuadamente el riesgo de tales productos y clientes, aceptaron esos productos sin desarrollar sistemas de gestión de riesgo adecuados.

Tecnología y pagos electrónicos — Los bancos desarrollaron y presentaron nuevos servicios y productos sin comprender del todo los riesgos LSB/ALD. Estos incluyen: tarjetas prepagas, banca a través de teléfonos celulares, tarjetas inteligentes, monederos móviles, y cloud banking. La dirección de los bancos debe asegurar que los riesgos LSB/ALD asociados estén claramente comprendidos y que los empleados estén entrenados respecto de los problemas de cumplimiento de la ley que plantea ese tipo de actividades.

Relaciones con terceros — Muchas acciones de cumplimiento hicieron mención de las relaciones con terceros. La dirección de los bancos debe asegurarse de desarrollar políticas, prácticas y procesos adecuados para mitigar los riesgos LSB/ALD asociados con este tipo de relaciones.

Políticas y prácticas de supervisión

La ley de Control de Lavado de Dinero de 1986 exige que los reguladores de los bancos:

- Prescriban regulaciones para exigir que los bancos establezcan procedimientos adecuados para asegurar y monitorear el cumplimiento LSB/ALD.
- Revisen los procedimientos LSB/ALD cuando realizan sus inspecciones.
- Informen al banco sobre los problemas hallados.
- Apliquen una acción de cumplimiento si el banco no establece procedimientos LSB/ALD o no corrige un problema previamente señalado.

En enero de 1987, la OCC desarrolló regulaciones para cumplir los requisitos de la Ley de Control de Lavado de Dinero de 1986. La 12 C.F.R. 21.21 (Código de Regulaciones Federales, por sus siglas en inglés) exige que un banco tenga un programa LSB/ALD escrito, que debe contener:

- Un sistema de controles internos LSB/ALD.
- Un sistema de inspección LSB/ALD independiente.
- Una persona designada responsable del monitoreo del cumplimiento LSB/ALD.
- Un programa de capacitación relacionado con LSB/ALD.

La subsiguiente Ley PATRIÓTICA de los EE.UU., promulgada en 2001, también exige que cada banco adopte un programa de identificación de clientes como parte del programa LSB/ALD.

En 2005, el Consejo Federal de Inspección de las Entidades Financieras (FFIEC, por sus siglas en inglés) desarrolló e implementó el Manual de Inspección Interinstitucional LSB/ALD. Dicho manual estandarizó los procedimientos de inspección para todas las agencias reguladoras de la actividad bancaria y aportó coherencia al proceso de inspección para los distintos tipos de entidades financieras. El manual fue revisado tres veces desde su publicación original para mantenerlo actualizado.

La OCC supervisa y monitorea el cumplimento LSB/ALD de los bancos, siguiendo los procedimientos de inspección del manual durante sus inspecciones. Los procedimientos están basados en los riesgos y se centran en las áreas de mayor riesgo del banco. Sin embargo, cada inspección incluye:

- Revisión de la evaluación de riesgos hecha por el banco.
- Revisión del programa del banco para asegurarse de que contiene:
  - — Controles internos
  - — Inspecciones independientes
  - — Capacidades e independencia del oficial LSB/ALD
  - — Capacitación
- Revisión de la efectividad del programa de cumplimiento de la Oficina de Control de Activos Extranjeros.

Como preparativo de una inspección, los inspectores analizan los datos LSB/ALD para comprobar si incluyen CTR (Informes de Transacción de Divisas, por sus siglas en inglés) y SAR (Informes de Actividades Sospechosas, por sus siglas en inglés) para planear las próximas inspecciones y determinar su alcance. Una inspección siempre se puede expandir hacia áreas con riesgos LSB/ALD más altos. Otra herramienta que usan los inspectores es el Sistema para el Riesgo Antilavado de Dinero, una herramienta de análisis que sirve para estudiar a los bancos y a las actividades de alto riesgo.

Capacitación

La OCC proporciona entrenamiento LSB/ALD a sus inspectores, organiza regularmente conferencias BSA y trabaja con el FFIEC, otros reguladores y la comunidad encargada de hacer cumplir la ley en el desarrollo de seminarios externos, conferencias y teleconferencias para la comunidad financiera. Esos seminarios y conferencias están diseñados para hacer frente a los nuevos problemas de lavado de dinero y financiación del terrorismo, y para proveer un foro de discusión sobre las últimas tendencias en lavado, tipologías criminales, ciberdelitos, fraude, financiación del terrorismo y otros esquemas delictivos.

Participación interinstitucional

La OCC trabaja con otros reguladores, con el FFIEC y con el Tesoro de los Estados Unidos para coordinar los esfuerzos LSB/ALD y para hacer frente a los problemas LSB/ALD a través de grupos de trabajo y varias fuerzas de tareas. Esos equipos incluyen:

- La Fuerza de Tareas para el Marco Antilavado de Dinero de los EE. UU. — liderada por el Tesoro — que revisa la legislación LSB/ALD y asegura su actualidad y relevancia.
- El Grupo Asesor para la Ley de Secreto Bancario (BSAAG) — presidido por la FinCEN — que coordina y discute los problemas ALD entre los reguladores y los agentes encargados del cumplimiento de la ley.
- El Grupo Delta del BSAAG, un grupo recientemente formado — presidido por la FinCEN y un representante de la industria de las finanzas. El grupo está formado por reguladores, miembros de la industria y agentes de cumplimiento de la ley. Tiene el objetivo

de reducir la variación entre los riesgos de cumplimento y de financiamiento ilícito, mientras que promueve un marco regulatorio más inteligente y eficiente.

- El Grupo de Trabajo BSA del FFIEC, formado por representantes de todas las agencias regulatorias, pensado para coordinar la consistencia en las inspecciones LSB/ALD y hacer frente a los nuevos problemas LSB/ALD.
- El Grupo de Trabajo Nacional Interagencias contra el Fraude Bancario — presidido por el Departamento de Justicia — está compuesto por miembros de las agencias reguladoras y de cumplimiento y tiene por objetivo combatir el fraude bancario.

Además de trabajar con esos grupos, la OCC realiza esfuerzos conjuntos con la Oficina de Terrorismo e Inteligencia Financiera del Tesoro de EE. UU., la FinCEN y la Oficina de Control de Activos Extranjeros, para hacer frente a los problemas LSB/ALD a nivel internacional. La OCC es anfitriona de varias escuelas LSB/ALD para reguladores extranjeros y participó en esfuerzos conjuntos en países extranjeros para hacer frente a los problemas de LSB/ALD. La OCC también brinda apoyo a la delegación de EE. UU. a la FATF (Grupo de Tareas para las Acciones Financieras, por sus siglas en inglés) en sus preocupaciones específicas sobre LSB/ALD.

Supervisión y Cumplimiento

El Controlador Curry se refirió luego a los procesos de supervisión y cumplimiento de la OCC. La OCC tiene dos grandes tipos de acciones que se pueden aplicar a los bancos que tienen programas LSB/ALD débiles o que no satisfacen los requisitos de cumplimiento: acciones informales y acciones formales.

Se aplica una acción informal cuando los problemas LSB/ALD tienen un alcance limitado y cuando la dirección del banco tiene un buen grado de compromiso y es capaz de corregir los problemas. Estas acciones generalmente no son públicas e incluyen cartas de compromiso, memorandos de entendimiento y asuntos que requieren atención del directorio.

Una acción de carácter formal es más severa, está autorizada por las leyes LSB/ALD y se da a conocer al público. Éstas incluyen órdenes de "Cese y Desista" (C&D), acuerdos formales escritos y multas civiles. Los acuerdos formales y las órdenes C&D exigen que el banco tome acciones específicas para corregir las deficiencias en su programa LSB/ALD. Las multas civiles pueden ser impuestas al banco, a sus funcionarios o directores, y a otras personas asociadas con el banco por no cumplimiento de las leyes y regulaciones LSB/ALD.

A pesar de que la severidad de una acción de cumplimiento queda generalmente a criterio de la oficina supervisora, hay algunos casos en que hace falta una violación de LSB/ALD para que la acción sea elevada al grado formal, generalmente una orden C&D. La Declaración Interinstitucional de Requerimientos de Aplicación LSB/ALD (Declaración Interinstitucional) declara que se extenderá una orden C&D cuando un banco tenga una violación de cumplimiento o cuando no ha corregido algún problema previamente identificado en el programa LSB/ALD. Las violaciones de cumplimiento incluyen:

- El banco no adopta o no implementa un programa de cumplimiento LSB/ALD escrito, que cubra adecuadamente los cuatro elementos requeridos: controles internos, inspecciones independientes, capacitación y designación de un oficial LSB/ALD.
- El programa LSB/ALD del banco tiene defectos en uno o más elementos, indicando que el programa o su implementación no son eficaces.

Los indicadores de un programa no eficaz pueden ser los siguientes:

- Un programa débil de Diligencia Debida de Cliente.
- Un proceso de identificación, monitoreo e informe ineficaz.
- Un proceso de evaluación de riesgos pobre.
- Un proceso de controles internos para las áreas de alto riesgo débil.

El Controlador Curry reconoció que en el caso en que un banco no haya corregido un problema previamente identificado, los reguladores saben que la acción correctiva puede llevar un tiempo considerable. Por lo tanto, la Declaración Interinstitucional y los reguladores no exigen que se extienda automáticamente un C&D cuando la inspección subsiguiente del banco muestra un "progreso sustancial aceptable" en la corrección del problema.

A efectos de la supervisión bancaria, la OCC tiene un proceso para asegurar que las acciones de cumplimiento sean justas, mesuradas y consistentes. Dicho proceso puede incluir las siguientes etapas:

- Durante la inspección en el lugar, hay una discusión preliminar entre los inspectores y la dirección del banco respecto de los hallazgos de la inspección.
- Los hallazgos se tratan con el inspector a cargo de la inspección global.
- Los hallazgos se tratan con el especialista en cumplimiento de la oficina supervisora del distrito.
- Los hallazgos se tratan con el Vice Controlador Asistente de la oficina supervisora local.
- Los hallazgos se tratan con el Comité de Revisión de Supervisiones del Distrito.
- Los hallazgos se tratan con el Comité de Revisión de Supervisiones de Washington.

Mejoras al proceso de supervisión

El Controlador Curry cerró su testimonio presentando las mejoras planeadas para el proceso de supervisión LSB/ALD. Declaró que la OCC está comprometida con un enfoque exhaustivo y detallado para el cumplimiento LSB/ALD y con una evaluación continuada y permanente del proceso de supervisión LSB/ALD. Las mejoras a los procesos incluyen:

- Revisar a nivel senior las acciones LSB/ALD complejas y de alto perfil.
- Incluir los hallazgos de LSB/ALD como un componente de la calificación de gestión según el sistema CAMELS.
- Mejorar el proceso de revisión para ofrecer distintas perspectivas y una respuesta más rápida a los problemas.
- Proporcionar una mayor flexibilidad para citar violaciones.
- Adoptar una visión más global del cumplimiento LSB/ALD de los bancos.

El Controlador Curry y el personal de inspección de la OCC reconocen la importancia de aplicar programas de cumplimiento eficaces en las entidades financieras de EE.UU. y el papel que cumple la OCC para asegurar que tales entidades no sean usadas para facilitar el lavado de dinero, el financiamiento del terrorismo y otras actividades delictivas. Los inspectores serán justos, escucharán y discutirán los problemas con los banqueros, y seguirán la misión declarada de la OCC. Dicha misión, desde 1863, es en parte la de "regular y supervisar los bancos para asegurar que operen de manera segura y sana". A

Thomas E. Nollner, director, Alvarez & Marsal Financial Industry Advisory Services in Houston, TX, USA, tnollner@alvarezandmarsal.com

Cumplimiento de la legislación antilavado de dinero en la industria de empresas de Servicios Monetarios

Las Empresas de Servicios Monetarios (ESM) — que incluyen los servicios de transferencia de dinero y de cambio de divisas — conforman una industria que mueve al menos varios miles de millones de dólares y que abarca desde negocios pequeños, operados por sus dueños, hasta sofisticadas organizaciones globales. El cumplimento de las leyes y regulaciones Antilavado de Dinero (ALD) se percibe fraccionado, con distintos grados de cumplimiento. Fortaleciendo tal percepción, la unidad de inteligencia financiera de Canadá, el Centro de Análisis de Transacciones Financieras e Informes de Canadá (FINTRAC, por sus siglas en inglés), bajo las leyes ALD de Canadá — o sea, la Ley de Ganancias por Actividades Delictivas (Lavado de Dinero) y Financiamiento del Terrorismo (PCMLTFA, por sus siglas en inglés) — ha estado penalizando cada vez más a las organizaciones que no cumplen con los requerimientos regulatorios y ha revelado públicamente sus nombres.

Bajo el mayor escrutinio de los reguladores, las ESM y sus asociados — incluyendo a los banqueros y a los correspondientes financistas — están examinando la industria de cerca y algunos están rehusando tener trato bancario o financiero con las ESM. Las ESM de Canadá, al comprender los riesgos de lavado de dinero y financiación del terrorismo, y la importancia creciente de gestionar su relación con sus asociados, están buscando conocer qué están haciendo sus colegas de la industria para encontrar soluciones.

El equipo antilavado (ALD) de Grant Thornton creó un informe de referencia a fin de ofrecer a las ESM y a las organizaciones financieras — ambas con objetivos de cumplimiento de ALD — una herramienta crítica para ayudarlas a evaluar los resultados de revisión de los programas de cumplimiento ALD, a conocer lo que la industria está realizando en la materia y, de manera más importante, a comprender los objetivos por los que debe luchar la industria de ESM.

Dicho informe de referencia puede ayudar a las ESM y a las entidades financieras a establecer los puntos de referencia de hoy y las metas futuras para los programas de cumplimiento antilavado.

Concretamente, el informe puede ayudar a

- identificar y evaluar la prevalencia de prácticas de cumplimiento en la industria de las ESM,
- determinar el impacto que pueden tener las prácticas específicas en la efectividad del programa de cumplimiento,
- establecer prácticas de cumplimiento efectivas y determinar la posición relativa de cada ESM dentro de la industria,
- gestionar las relaciones de las ESM con las entidades financieras asociadas,
- regular las prácticas de cumplimiento en la industria y
- evaluar el ritmo de progreso de los cambios.

Perfil de la población de ESM

La mayoría de las ESM incluidas en la población de referencia ofrece servicios de envío de dinero, y casi la mitad de ellas ofrece también servicios de cambio de divisas. Otros servicios incluyen cambio de cheques, órdenes de pago y préstamos de día de pago. Muchas ESM proporcionan muchos de esos servicios.

Dentro de las ESM que ofrecen servicios de envío de dinero, comprobamos que la mayoría atiende una región geográfica específica, mientras que una porción significativa (algo más de un cuarto de todas las ESM que disponen de dichos servicios) envía dinero a amplias regiones del mundo — o bien usando redes mundiales establecidas o usando redes de su propiedad.

El informe también analizó la población de referencia para entender cómo las ESM interactuaban con sus clientes. La proporción de empresas que ofrecía acceso en línea a sus clientes era sólo del 2 por ciento, el 48 por ciento interactuaba solamente a través de encuentros personales cara a cara, y el 50 por ciento ofrecía

formas múltiples de acceso. Las entidades que ofrecían tipos de interacción múltiples brindaban acceso completo sólo después de un encuentro cara a cara.

A continuación, presentamos un resumen de las principales áreas que usamos como referencia:

Oficial de cumplimiento

Independientemente de si el oficial de cumplimiento de la entidad era el dueño o un empleado, no había diferencias discernibles entre tener registros e informar sobre deficiencias. Sin embargo, sólo un pequeño porcentaje de los oficiales de cumplimiento tenían credenciales ALD relevantes, tales como CAMS (siglas en inglés para Especialista Certificado en Antilavado de Dinero). Vemos que esto ya está cambiando porque cada vez son más los oficiales de cumplimiento que buscan entrenamiento y certificación.

Si bien había muchas ESM donde la función de cumplimiento estaba a cargo de una sola persona, las ESM más grandes tenían recursos para mantener un equipo. Sorprendentemente, notamos que las deficiencias en los registros y en los informes eran más frecuentes cuando el oficial de cumplimiento estaba asistido por un equipo. A pesar de tener un equipo puede ser beneficioso para la organización, el oficial de cumplimiento necesita asegurar que la calidad y la consistencia se mantienen siempre altas.

Evaluación de riesgos

El documento de evaluación de riesgos en sí mismo tiene que ser la base del programa de ALD de toda organización. Una buena evaluación de riesgos documenta los riesgos de lavado y financiación del terrorismo específicos de su negocio individual e incluye controles para mitigarlos. Una vez que usted ha identificado sus mayores riesgos, asegúrese de estar monitoreando activamente a los potencialmente peligrosos clientes y transacciones. Protéjase y proteja a su negocio mediante la ejecución de los controles documentados, incluyendo la averiguación de la proveniencia de la información sobre los fondos antes de hacerse responsable de facilitar la transacción.

Si bien la mayoría de las entidades que revisamos tenía documentada una evaluación de riesgos, muchas estaban todavía en el proceso de hacer del documento una realidad práctica; el 84 por ciento no había identificado ninguna área de alto riesgo en su evaluación. Inesperadamente, notamos que aquellas que sí las habían identificado demostraron menor probabilidad de identificar y denunciar las actividades sospechosas al FINTRAC. En algunos casos, vemos que la identificación de áreas de mayor riesgo funciona realmente como control preventivo, pues los clientes y transacciones de alto riesgo se identifican enseguida y se rechazan desde el principio, limitando la exposición de la entidad a las actividades de lavado.

Capacitación

La incorporación de evaluaciones como parte de un programa de Entrenamiento de ALD puede asegurar la comprensión de los requerimientos y mantener en casa los dólares que usted invirtió en la capacitación de su personal. Según nuestro estudio, menos de un cuarto de las ESM habían incorporado un sistema de evaluaciones a su programa de entrenamiento.

Conviene mantener una adecuada documentación de las capacitaciones en curso respecto de los requerimientos del programa de cumplimiento. Ahora hay muchos recursos a medida de las ESM para que las empresas puedan acceder en línea. Dichos recursos también sirven para conocer los resultados de las evaluaciones y comprobar que los empleados las hayan completado.

La capacitación también debería incluir material relevante para la función que el empleado cumple en la empresa, y debería brindar una buena comprensión de las acciones ALD, junto con los conocimientos específicos necesarios para que pueda cumplir bien su parte en la estrategia de ALD. Actualmente, se espera que la capacitación esté adaptada al puesto y a la función de su personal.

También es importante revisar con su personal los requerimientos específicos para efectuar los registros. A usted le conviene usar ejemplos tomados de su organización para que esta acción sea efectiva.

Registros

Si bien la mayor parte de las ESM mostraron una buena comprensión de los requerimientos ALD, una alta proporción — 76 por ciento — evidenciaron deficiencias en los procedimientos de registro. Las deficiencias más habituales fueron:

- El personal no tenía claros los requerimientos específicos para los registros,
- no se obtenían los datos sobre la ocupación o los datos documentados no eran claros
- no se recogía información sobre los beneficiarios corporativos ni se la documentaba, y
- no se investigaba si la transacción se hacía a nombre de un tercero o de alguna Persona Políticamente y Foránea Expuesta (Politically Exposed Foreign Person — PEFP).

Transacciones sospechosas

Si bien la mayoría de las ESM comprendieron bien la importancia y la necesidad de denunciar las transacciones sospechosas, la mayor parte de ellas nunca envió un Informe de Transacción Sospechosa (STR por sus siglas en inglés). Las entidades que sí lo hicieron generalmente eran más grandes y tenían un sistema automatizado para ayudar a identificar patrones de transacción inusuales.

Es muy importante que todo el personal (del mostrador, de las oficinas interiores / de procesamiento y gestión) tenga conciencia y esté adecuadamente capacitado para reconocer las señales de alerta (red flags) de una transacción inusual que induzca sospechas de lavado de dinero o financiación del terrorismo.

Los resultados de nuestra investigación indican que los programas de cumplimiento antilavado están empezando a producir los resultados deseados. Sin embargo, también se evidencia que muchas ESM tienen que empezar a centrarse en la identificación de transacciones potencialmente sospechosas. Quizás sólo se requiera una evolución en el ejercicio del régimen de cumplimiento, ahora que el resto de los elementos del programa está en su lugar.

Sobre todo, las entidades financieras que trabajan con clientes de alto riesgo necesitan implementar y mantener transparencia para sus clientes de banca. Tener un programa de disuasión riguroso y efectivo para prevenir el lavado de dinero y el financiamiento del terrorismo es un factor crítico de éxito para las Empresas de Servicios Monetarios de hoy.

La industria de ESM de Canadá es un segmento vital para muchas culturas y para quienes no están bancarizados. También ofrece métodos alternativos y competitivos para transferir fondos. La industria seguirá enfrentando sus propios desafíos pero con una mejor comprensión de los requerimientos regulatorios que la industria ha de desarrollar. También se va a distinguir a aquellas ESM que acaten los requisitos — o los excedan con celo — especialmente los que sirvan para identificar transacciones sospechosas.

Para más información, o para leer el informe completo, le invitamos a visitar www.GrantThornton.ca/AML

Patrick Ho, of CPA, CA, CBV, CAMS, senior manager, Grant Thornton, LLP, Toronto, ON, Canada, Patrick.Ho@ca.gt.com

Jennifer Fiddian-Green, CA.IFA, CMA, CFI, CFE, CAMS, partner, Grant Thornton, LLP, Toronto, ON, Canadá, Jennifer.Fiddian-Green@ca.gt.com

CON LAS MANOS EN LA MASA

Béisbol, fútbol americano, baloncesto, hockey, fútbol y lacrosse son deportes de equipo. Aunque cada deporte sea diferente el objetivo es el mismo — ganar. Hay algo en común a todos estos deportes cuando dos equipos se enfrentan en un campo de juegos. Tener el equipo más talentoso no significa siempre que se gana, aunque seguramente favorezca. Tener el equipo más preparado resulta más ventajoso. A la hora de la verdad, cuando hay que decidir, la preparación puede triunfar sobre el talento. El equipo más talentoso, si no está preparado, seguramente jugará con falta de enfoque y de disciplina. El equipo mejor preparado se inclina más a seguir su plan de juego y a explotar las vulnerabilidades de sus oponentes. Cometerá menos errores, con lo cual impedirá que su oponente explote sus vulnerabilidades. Así, el equipo mejor preparado tendrá mayores posibilidades de salir triunfante.

Si se compara el fraude con un evento deportivo y opone el estafador al investigador, el jugador que ganará es habitualmente el mejor preparado. Frecuentemente los estafadores son los jugadores más talentosos. Tienden a ser proactivos y se encuentran motivados por la codicia y la arrogancia. Con la mayor frecuencia, tienen la ventaja de ser proactivos mientras que los investigadores son reactivos. Sin embargo, cuando los investigadores se preparan y planifican cómo enfrentarse al adversario, tienen mayores posibilidades de explotar las vulnerabilidades del estafador. Tales vulnerabilidades empiezan con la avaricia y la arrogancia del estafador. Los investigadores deben entender el delito, saber cómo operan los estafadores y explotar las vulnerabilidades del villano adversario. Al hacerlo, la posibilidad de llevar a cabo una investigación exitosa aumenta notoriamente.

Investigadores de cumplimiento de la ley y de fraude del sector privado

Las investigaciones sobre el fraude van de lo simple a lo complejo. Se encuentre usted en la aplicación de la ley o en el sector privado, la metodología para llevar a cabo investigaciones sobre fraudes tendría que ser la misma. Conviene que dé los pasos investigativos apropiados para identificar la actividad sospechosa, compruebe la existencia del fraude, minimice la pérdida financiera y eleve al máximo el potencial de recuperación de los activos. Algunas herramientas investigativas son semejantes en ambos grupos, pero cada grupo tiene sus propias herramientas únicas. Por ejemplo, los que se ocupan de la aplicación de la ley tienen la destreza de obtener pruebas por medio de citaciones de un gran jurado y órdenes de allanamiento, como también la capacidad de hacer arrestos. Los investigadores del sector privado tienen acceso a la gama total de informes de su institución así como la ventaja de poder obligar a los empleados a decir la verdad durante las entrevistas al riesgo de cesantía. La mayor diferencia entre los que aplican la ley y el sector privado es el objetivo final de la investigación. Para quien aplica la ley, el objetivo consiste en desarrollar pruebas que resulten en el enjuiciamiento del delincuente y la confiscación de activos. Para los investigadores del sector privado, el objetivo consiste en proteger la reputación e integridad de la institución, impedir o minimizar pérdidas financieras y recobrar activos que se le atribuyen al fraude.

Preparación y planificación

Al preparar una investigación sobre fraudes, el investigador tiene que entender el delito. ¿Cuál es la naturaleza del fraude? ¿Cuáles son los elementos de la actividad sospechosa o delictiva? ¿Se extiende el fraude por debajo de la superficie? ¿Qué medidas investigativas deben tomarse para identificar la actividad sospechosa o para probar el fraude? Los investigadores de delitos tienen que conocer las leyes que se pueden aplicar y qué nivel de prueba es necesario para probar violaciones en un juicio. Los investigadores de fraudes del sector privado tienen que tener el conocimiento de las políticas y procedimientos institucionales y de los pasos investigativos para mitigar el fraude.

Independientemente de lo simple o complejo que parezca la trama del fraude, los investigadores siempre tendrían que preparar un plan investigativo por escrito. El plan tendría que incluir la predicción de la investigación o los factores que justifican la investigación los elementos que deben comprobarse, las consideraciones logísticas tales como el personal y el equipo necesario, los pasos investigativos que se han de tomar y planes de contingencia. Todos los planes investigativos tendrían que incluir contingencias para enfrentarse con lo conocido y lo desconocido, así como lo esperado y lo inesperado. La planificación para investigaciones complejas tiene mayor significado; sin embargo, planificar para fraudes más sencillos tiene igual nivel de importancia.

Al llevar a cabo investigaciones sobre fraudes, especialmente tramas que se convierten en escenarios complejos, resulta fácil desenfocar y alejarse de la investigación que se tenía en mente. Por ello resulta importante planificar. Los investigadores deberían mantener disciplina investigativa y seguir el plan escrito. Esto ayuda a mantenerse enfocado en el tema. Los investigadores deberían estar vigilantes cuando evalúan e investigan una trama de fraude para determinar si hay más que lo que aparece a primera vista. ¿Es más complejo el fraude? ¿Está el fraude vinculado a otros? ¿Cómo se manejan las contingencias? Planes investigativos integrales ayudan a contestar estas y otras preguntas.

Comprender el problema del delito

Una parte importante de la preparación consiste en comprender el problema del delito. El fraude tendría que ser evaluado y entendido desde dos perspectivas: la genérica y la específica. Desde la perspectiva genérica y más simplista, el fraude es un engaño intencional. La habilidad de engañar y de evitar que se le detecte a uno es la primera clave del éxito del estafador. Hay una miríada de fraudes diferentes. Como se mencionó antes, van desde lo simple a lo complejo. Además de entender el fraude de manera general, resulta imperativo que los investigadores comprendan las tramas de fraudes específicos que encuentran tanto como aquellos a los que se encuentran vulnerables. Cuando los investigadores entienden cómo los estafadores aprovechan las tramas de fraudes genéricos y específicos, se posicionan para preparar y planificar contra los estafadores de manera más efectiva y eficiente.

> Un mecanismo que mejora la comprensión es la capacitación

Un mecanismo que mejora la comprensión es la capacitación. Como herramienta de capacitación, los investigadores deberían estudiar tipologías de casos de fraudes. Tales estudios de caso permiten discernir cómo los estafadores operan y explotan vulnerabilidades sistemáticas para perpetrar sus fraudes. Las lecciones aprendidas de investigaciones previas son una buena herramienta de aprendizaje. Una gran fuente de tipologías de casos es la de expedientes judiciales incluyendo acusaciones, información, acuerdos judiciales y otros dictámenes acusatorios. Estos expedientes jurídicos habitualmente tienen una relación de hechos que delinea la actividad delictiva. Estudiar tipologías de casos resulta un mecanismo excelente para comprender el problema del delito.

La mejor manera para comprender el problema del delito de fraude es a través de la experiencia investigativa de primera mano. Mientras más experiencia tenga el investigador, mejor equipado estará para enfrentarse al fraude. Aprender de la experiencia investigativa es una herramienta poderosa. Algo que tendrían que aprender todos los investigadores es a depender de su intuición investigativa, especialmente cuando se enfrentan al engaño del fraude. Los investigadores deberían confiar en sus instintos. Tendrían que comparar y evaluar los hechos del caso

que manejan a los hechos desarrollados en su experiencia anterior que respaldan sus instintos. Si una situación no parece razonable, confíe en sus instintos. No acepte explicaciones hasta que se encuentre satisfecho con la razonabilidad de la representación.

Compitiendo con el estafador

¡Empezó el juego! Usted ha preparado y planificado la investigación y comprende el problema del delito. Llegó el momento de enfrentarse al adversario y de investigar al estafador. Ganar el juego o tener éxito en la investigación depende de cómo usted maneje los factores siguientes:

- Ventajas
- Trama y engaño
- Intimidación
- Persistencia
- Análisis (razonabilidad)
- Estrategia de salida

Ventaja

Un buen estafador siempre quiere tener ventaja y dictar el ritmo del juego. Hay maneras sutiles de hacerlo. El estafador quiere estar en control y en la mayor parte de las veces se considera más inteligente que los investigadores. Deje que el estafador piense que lleva ventaja. Él quiere que usted sepa que el es más inteligente que usted. Si usted le permite mantener la impresión de que lleva ventaja, invariablemente bajará la guardia y hablará. Use su destreza de comprensión auditiva y deje que hable. Puede ser lo que hace que el estafador se pierda.

Trama y engaño

El villano adversario ha hilado una tela de engaño para facilitar su trama de fraude. Sea paciente, disciplinado y meticuloso. En algún momento, el peso del engaño se desmoronará sobre el estafador. Las tramas de fraude tienden a hacerse más complejas y difíciles de mantener a medida que crecen. En algún punto comenzarán a desentrañarse.

Intimidación

Llegará el momento cuando usted le preguntará al estafador una pregunta que tocará la cuerda sensible o amenazará con exponer la trama y el engaño. La respuesta habitual en este momento será defensiva e intimidatoria. Su adversario lo atacará. El estafador le hará saber que su pregunta fue estúpida y una pérdida de su valioso tiempo. Será condescendiente intentando mantener la ventaja a través de la intimidación. Esta es una señal de que usted se encuentra en el camino acertado y de que su adversario se encuentra contra las cuerdas. En este punto el investigador debe perseverar.

Persistencia

A medida que avanza el juego, habrá más trama y engaño para cubrir las grietas en el marco del fraude. La situación podría complicarse y hacerse más desafiante para el estafador. Como investigador, tiene que ser persistente. Siga preguntando y rompa la fachada de la estafa. Sea persistente y meticuloso al armar su caso jurídico — sea éste delictivo o interno. Mientras más persistente el investigador, mayores probabilidades hay de ganar el juego.

Análisis

El análisis respalda la persistencia. Hay una variedad de herramientas analíticas disponibles para los investigadores. Lleve a cabo análisis integrales para romper la trama y el engaño. Pregunte continuamente sobre la razonabilidad de las representaciones que le ofrecen. En algún punto el análisis y la razonabilidad pesarán más que la trama y el engaño.

Estrategia de salida

Tenga presente que durante este proceso un buen estafador tiene una estrategia de salida. Cuando la trama del fraude está por desentrañarse, muchos estafadores ejecutan su estrategia de salida. No se deje sorprender. Esté preparado para ocuparse de la estrategia de salida del estafador. Las estrategias de salida varían. Algunos estafadores quieren que se les capture porque el peso de su fraude es excesivo, mientras que otros son tan arrogantes y codiciosos que se enceguecen ante el hecho de que el final está a la vista. Algunos estafadores siguen siendo disciplinados y centrados y tienen lo que consideran un abrigo seguro donde podrían guarecerse.

Último juego

Tenga presente que habrá un último juego. Esto tendrá que aparece en su plan investigativo escrito. Para los investigadores de delitos, el último juego es una acción penal y confiscación de activos. Para el investigador del sector privado, el último juego consiste en proteger los activos de la institución y su reputación. Si los investigadores de delitos y del sector privado tienen éxito, habrán privado a los estafadores de su estrategia de salida y último juego de vivir felices y comer perdices con los resultados de su delito.

Cuando los buenos de la película vencen a los malos, independientemente del talento de los malos, generalmente se debe a la preparación de los buenos, su comprensión del delito y la ejecución del plan de juego.

Dennis Lormel, presidente y CEO, DML Associates, LLC, Lansdowne, VA, EE.UU., dlormel@dmlassociateslic.com

ACAMS Recognition Awards 2013

ACAMS presents three awards to recognize individuals who have made a significant, positive impact on the financial crime industry.

ACAMS
AML Professional of the Year

Nominate your peers who have contributed significantly to AML/CTF and financial crime prevention. One member will be honored in Las Vegas as the ACAMS AML Professional of the Year for 2013. Submit nominations online at acamsglobal.org by July 31.

ACAMS
Al Gillum
Volunteer
OF THE YEAR

Each year, we hand-select an individual to be honored with the Al Gillum Volunteer of the Year Award. The honoree is recognized for generously donating their time and expertise to ACAMS and for contributing to chapter development, training events, and overall member growth.

ACAMS TODAY
Article of the Year

This award recognizes those who support the ACAMS mission of providing valuable editorial content to its members. Recognize the author of your favorite *ACAMS Today* article. Please send your nomination to editor@acams.org by July 31.

2012 ACAMS Recognition Award Winners

AML Professional of the Year

James Candelmo, CAMS
Ally Financial Services

Al Gillum Volunteer of the Year

Vasilios P. Chrisos, CAMS
Macquarie Compliance Macquarie Group

ACAMS Today Article of the Year

Kevin Nash, CAMS, CFE, CIPP
Capital One Financial

ACAMS Today Article of the Year

Dorina Vornicescu, CAMS
KPMG

Cuánto vale su evaluación de riesgos?

La edición de 2010 del Manual de Inspección de Antilavado del Consejo Federal de Inspección de Entidades Financieras (FFIEC, por sus siglas en inglés), que responde a la Ley de Secreto Bancario/Antilavado de Dinero — LSB/ALD), se destaca por una importante expansión de la parte dedicada a la evaluación de riesgos, dentro de su Esquema General de Procedimientos de Inspección. Este es un paso crucial en la promoción de un marco básico para la aplicación de un programa efectivo de cumplimento de LSB/ALD. El hecho de que el FFIEC haya puesto tanto énfasis en esta sección y que la haya ubicado muy cerca del principio no es una casualidad. La función y el valor de la evaluación de LSB/ALD no puede ser subestimada, por su impacto directo en el programa de cumplimiento LSB/ALD y en el manejo del riesgo de cumplimiento. Esto tiene relación especial con la eficacia del monitoreo de las transacciones, la denuncia de actividades sospechosas y la asignación de recursos dentro de la infraestructura de cumplimento de la entidad. Independientemente de si la entidad financiera aplica formas manuales o automatizadas para el monitoreo de transacciones y para los sistemas y controles de investigación de casos; la evaluación de riesgos de LSB/ALD y, más específicamente, la implícita evaluación del riesgo de *cliente* es la piedra angular que sostiene todos los esfuerzos para identificar, medir, monitorear y denunciar actividades de lavado de dinero y de financiamiento del terrorismo. En general, la seriedad de la evaluación de LSB/ALD aumentará en proporción directa a la escala y a la complejidad de las operaciones de las empresas. Tanto para los pequeños bancos comunales como para las grandes entidades financieras multinacionales con Unidad de Inteligencia Financiera (UIF) dedicada, la evaluación de los riesgos es vital para implementar las iniciativas de ALD.

Por mera coincidencia — o no — lo dicho también es válido para la influencia que pueden tener las evaluaciones de riesgo sobre la capacidad de las autoridades encargadas de aplicar la ley para detectar, investigar y enjuiciar eficazmente las actividades de financiamiento del terrorismo; y para asignar recursos para la revisión y análisis de los Informes de Transacción de Divisas (CTR, por sus siglas en inglés) y los Informes de Actividad Sospechosa (SAR, por sus siglas en inglés). Por lo tanto, es lógico pensar que la evaluación de riesgo de LSB/ALD representa tanto un *valor de costo* como un factor de costo agregado, tanto para las entidades financieras como para los organismos encargados de aplicar la ley, en términos de dinero real. Para explicar mejor esta hipótesis, vamos a explorar el tema más a fondo.

La guía para la inspección de LSB/ALD define la tarea de evaluación de riesgo como un proceso de dos pasos. Paso uno: identificar los productos, servicios, clientes, entidades y ubicaciones geográficas específicos del banco. Paso dos: en un análisis más detallado de los datos obtenidos en el paso uno, evaluar las datos de las actividades del banco, en relación con el Programa de Identificación de Clientes (CIP, por sus siglas en inglés) y en relación con la información de la auditoría previa del cliente (CDD, por sus siglas en inglés); señalando que dentro de cualquier tipo de producto o categoría de cliente habrá titulares de cuentas que presentan *distintos niveles de riesgo*.[1] Las iniciativas de CIP, CDD y de Debida Diligencia Mejorada (EDD, por sus siglas en inglés) forman parte de los procedimientos de "Conocer a Su Cliente" (KYC, por sus siglas en inglés) y son las herramientas esenciales para completar dicho procedimiento de dos pasos. A los efectos de este estudio, nos centraremos en el paso dos.

Calificación de riesgo de las entidades financieras, Diligencia Debida Mejorada (EDD) y eficiencia de los recursos

Desde la perspectiva del paso uno de la entidad financiera, una evaluación de LSB/ALD bien documentada y basada en los riesgos ayudará a identificar el perfil de riesgo de la institución y servirá como base para un programa de cumplimiento que sostenga los "cuatro pilares" efectivos del cumplimiento de LSB/ALD. Estos son: designación de un oficial de LSB/ALD; establecimiento de controles internos; testeos independientes; y capacitación. Desde la perspectiva del paso dos, sin embargo, una evaluación de LSB/ALD bien desarrollada — especialmente el componente "riesgo de cliente" — servirá de guía para identificar y descalificar a los clientes con demasiada probabilidad de quedar sujetos a monitoreos más frecuentes y exhaustivos. La evaluación del riesgo tiene gran peso para el CIP (Programa de Identificación de Clientes) a través de la determinación de un perfil de riesgo de cliente bien exacto en el momento de recoger los datos para la apertura de una cuenta y para los esfuerzos de Diligencia Debida del Cliente (CDD).

Las políticas, procedimientos y procesos de CDD eficaces son la piedra angular de un programa de LSB/ALD sólido.[2] Es en este punto que una entidad debe determinar la calificación de riesgo de cliente. La calificación puede expresarse con valores numéricos o con un puntaje RAV (Rojo, Amarillo, Verde) para clasificar las categorías de escalamiento de EDD en los entornos de operación manual, o bien asignando un puntaje numérico como parte del Archivo de Información del Cliente (CIF, por sus siglas en inglés), cuando las operaciones están automatizadas. Tanto en condiciones de operación manual como de operación automatizada, hay que hacer una Diligencia Debida Mejorada (EDD) a los clientes

[1] Manual de Inspección de Antilavado del Consejo Federal de Inspección de Entidades Financieras (FFIEC), *Evaluación de riesgos LSB/ALD* – Resumen, páginas 22-30.
[2] Manual de Inspección Antilavado del Consejo Federal de Inspección de Entidades Financieras (FFIEC), *Diligencia Debida de Cliente* (CDD – Customer Due Diligence) – Resumen, página 63.

de mayor riesgo, para establecer procesos y controles defectivos que mitiguen los riesgos de LSB/ALD. Si no se controlan adecuadamente, las calificaciones de riesgo ineficaces o inexactas tienen un impacto directo y sostenido en los esfuerzos de monitoreo de clientes y transacciones (EDD/KYC), a lo largo de toda la relación con los clientes, con la consecuencia involuntaria de retrasar o, peor aún, de anular toda capacidad para detectar actividades inusuales potencialmente sospechosas.

Una vez que ese segmento de clientes fue identificado, aislado y escalado a un nivel superior de monitoreo, surge la pregunta de si se asignaron suficientes recursos humanos y tecnológicos para asegurar que la empresa pueda ejecutar una estrategia de cumplimiento de LSB/ALD que satisfaga las metas críticas de desempeño y las correspondientes obligaciones regulatorias. Aquí se ve cómo una ineficaz evaluación de riesgo de cliente tiene correlación directa con la asignación de los recursos, la eficiencia y la eficacia, independientemente del entorno operativo (manual vs. automatizado). Para las entidades financieras, la evaluación del riesgo/evaluación del riesgo de cliente afecta cuatro componentes de sus costos:

1) la capacidad para identificar y medir la actividad sospechosa, o sea, la capacidad de erradicar las cuentas y las relaciones peligrosas;

2) el costo directo de los recursos humanos dedicados a EDD/KYC y la suficiente capacidad de las iniciativas de monitoreo de transacciones;

3) el impacto del costo-beneficio directo de las soluciones informáticas relacionadas con la exactitud en la predeterminación de los parámetros y en los esfuerzos de ajuste/reajuste; con la exactitud para identificar actividades y patrones sospechosos; con la gestión de los costos de proveedores; y con

4) la capacidad para encarar nuevos productos y servicios adecuados al perfil o necesidades de los clientes.

En términos prácticos, los costos mencionados equivalen a pérdidas en dinero real, a través de: relaciones indeseadas; apertura de cuentas de alto riesgo; incapacidad para identificar las actividades sospechosas, lo que resulta en potenciales acciones regulatorias que incluyen multas y restricciones; pérdida de oportunidades de negocios; escasez de personal, que debilita la efectividad de los programas LSB/ALD; *exceso de personal* que infla los costos y/o produce una mala asignación de valiosos recursos que podrían haberse dedicado a mejorar los programas o los sistemas; y clientes de alto riesgo que "se cuelan por las grietas". Al final, las entidades financieras que tienen una evaluación de riesgos débil deberán afrontar muchos peligros, que incluyen riesgos de cumplimiento, legales, operacionales y de reputación, que no se agotan en esta lista.

Entidades financieras vs. autoridades de aplicación de la ley: contrastes y paralelismos

Si bien las entidades financieras tienen un grupo de clientes individuales y una capacidad de calificar sus riesgos, basada en las transacciones y en los Archivos de Información de Clientes (CIF) — que equivalen a datos duros — las autoridades de aplicación de la ley, para construir sus casos y procesarlos judicialmente, dependen de informaciones provenientes de un grande y variado pool de recursos. Las autoridades dependen de la calidad de la información — tanto de fuentes internas como externas — y se encuentran con lagunas de información inherentes porque, si bien pueden averiguar que cierto número de organizaciones criminales, lavadores de dinero o posibles entidades de financiación terrorista residen en una determinada jurisdicción, no

pueden averiguar mucho más. La mayoría de los descubrimientos surgen de otras investigaciones sobre el delito precursor. Por eso, la información que las entidades financieras envían a las autoridades debe ser clara y eficaz. Para las autoridades, muchos casos comienzan con una pequeña información sobre una red financiera ilícita que debe ser procesada judicialmente. Dentro de la comunidad financiera, sin embargo, los clientes generalmente tienen que proporcionar una cantidad considerable de información antes de que puedan usar productos y servicios, y las entidades tienen la oportunidad de analizar toda la actividad de los clientes a lo largo de su relación comercial.

Por lo tanto, es lógico pensar que, por el lado de la entidad financiera, el resultado final de una base ineficaz de evaluación de riesgos de LSB/ALD, con sus correspondientes datos CIP, DDD, EDD/KYC; impacta finalmente en el lado de la ecuación correspondiente a las autoridades, a través de información parcial, incompleta o faltante en los Informes de Transacción de Divisas (CTR) y en los Informes de Actividades sospechosas (SAR). No identificar el carácter de alto riesgo de un cliente a través de CIP, CDD y EDD puede resultar en la pérdida de pistas tempranas en las investigaciones criminales. No marcar un cliente como de alto riesgo por actividad sospechosa ni mantener esfuerzos sólidos de EDD/KYC a través del monitoreo de cuentas y transacciones puede significar la pérdida de información crítica para construir o fortalecer las causas penales en curso. Los Informes de Transacción de Divisas y de Actividades Sospechosas inexactos, incompletos o sin presentar pueden resultar en pistas incorrectas, facilitación no intencional de financiamiento de actividades criminales o terroristas y la pérdida de las oportunidades de enjuiciamiento penal.

Desde el punto de vista de las autoridades, los escenarios de manejo de casos reflejan los desafíos que enfrentan las entidades durante el paso dos del proceso de evaluación de riesgo respecto de las iniciativas EDD/KYC, pero en un contexto de tiempos extendidos y de un gran número de pools de información. Hay que considerar que la evaluación de riesgo/evaluación de riesgo de cliente de la entidad financiera impacta cuatro componentes de costo clave para las iniciativas de aplicación de la ley:

1) la capacidad de identificar y medir la actividad delictiva, o sea la habilidad de erradicar las cuentas de financiación, las organizaciones y las relaciones más viles;

2) el costo directo de los recursos humanos dedicados a monitorear e investigar las iniciativas relacionadas con el nivel de dotación de personal y horas-hombre dedicadas;

3) el impacto del costo-beneficio directo de las soluciones informáticas relacionadas con el aumento en la precisión para identificar las actividades y patrones más sospechosos; y

4) la capacidad de las autoridades para construir y explorar oportunidades para crear fuerzas de tarea conjuntas — regionales, domésticas y multinacionales — que se ocupen específicamente de las organizaciones criminales, de lavado y de financiamiento del terrorismo "de más alto riesgo". Las agencias de aplicación de la ley pueden necesitar aproximadamente el mismo tiempo para resolver casos relativamente pequeños como el que necesitan para los más grandes. Por lo tanto, la asignación de recursos es crítica para el éxito de los procesamientos a escala general.

Para las autoridades responsables de hacer cumplir la ley, los costos mencionados pueden equivaler a pérdidas millonarias, a través de: apertura y prosecución de casos e investigaciones de bajo riesgo, que resultan en el desperdicio de valiosos recursos y oportunidades de investigación; falta de identificación de las tendencias criminales, que resulta en un potencial crecimiento de dichas tendencias y pérdidas futuras para las instituciones; oportunidades procesales perdidas y recursos judiciales mal asignados; recortes de personal o de recursos que debilitan el impacto y la efectividad de las investigaciones; *exceso de personal* que infla los costos y/o provoca una mala asignación de fondos valiosos que podrían haberse dedicado para mejorar o actualizar los programas; criminales de alto riesgo y terroristas que "se cuelan por las grietas".

Por eso, las evaluaciones de riesgo LSB/ALD ineficaces por parte de las entidades financieras representan un riesgo operativo considerable para la comunidad responsable de la aplicación de la ley. Al igual que los bancos, las autoridades también tienen recursos limitados y deben tratar de utilizar sus activos eficientemente para obtener el mayor impacto y beneficio posibles. Los procesos de gestión y evaluación del riesgo son metodologías de mitigación de riesgos incuestionablemente probadas, tan útiles para las entidades financieras como para las autoridades que hacen aplicar la ley, pero las autoridades de los EE. UU. tuvieron que luchar para implementar este criterio, ya que hubo poca o ninguna presión para adoptarlas. Parte del problema puede ser que acaso las metodologías de referencia no son consideradas como opción, o no fueron presentadas como tales.

Las autoridades encargadas de hacer cumplir la ley dependen del acceso a los individuos denunciados en los Informes de Transacción de Divisas (CTR) y los Informes de Actividades Sospechosas (SAR). Es tarea de las autoridades analizar esa información y es ahí donde las evaluaciones de riesgo y la priorización de sujetos podrían revolucionar la manera en que los lavadores de dinero se identifican y persiguen en los Estados Unidos y en otros países. Muchas autoridades confían en los SAR porque las entidades financieras ya han identificado a los sujetos ahí denunciados que requieren mayor investigación. Este método no toma en cuenta ninguna de las informaciones a la que las autoridades tienen acceso ni considera los individuos y entidades sospechosas que infiltran muchas instituciones. Hay grandes volúmenes de inteligencia entre los datos LSB que están a disposición de casi todos los departamentos responsables del cumplimiento de la ley en los Estados Unidos, pero el mero análisis de los SAR señala dos tipos de criminales, aunque no todos los sujetos de los SAR sean criminales. Un tipo de delincuente, que es el más común, es aquél que no está suficientemente experimentado como para evitar la detección y los controles; el otro tipo incluye a quienes son demasiado grandes como para esconderse detrás de su actividad. Los lavadores de dinero experimentados, que han aprendido a recolocar sus fondos silenciosamente en la sociedad pueden nunca aparecer en un SAR, pero es mucho más probable que sean identificados en los Informes de Transacción de Divisas (CTR).

Resumen

Tanto las entidades financieras como las autoridades de aplicación de la ley deben lidiar con la organización y la estructuración de una vasta flota de información, a través de la asignación eficaz de los recursos humanos y de la tecnología informática. Cuando las autoridades pueden combinar los datos que acumularon con los datos que produce la comunidad financiera, se genera una probada capacidad para desarrollar una inteligencia proactiva de clase mundial y para realizar incursiones significativas dentro las comunidades de lavado de dinero y de financiación del terrorismo. De esa manera, el Tesoro de los Estados Unidos, la FinCEN (Red de Prevención de Delitos Financieros) y otros cuerpos regulatorios globales pueden a su vez estar más informados sobre los patrones y tendencias en curso para guiar mejor a la comunidad financiera en la prevención y disuasión del mal uso de las redes financieras globales y de los Estados Unidos.

Brian Arrington, MBA, CAMS, director de comunicaciones del Capítulo de Chicago de ACAMS, examinador con el Federal Reserve Bank de Chicago, Chicago, IL, EE.UU.

Clayton Byford, CAMS, analista financero contra amenazas, Chicago HIDTA/HIFCA, Chicago, IL, EE.UU., cbyford@chicago-hidta.org

Lisa M. Grigg, CAMS:

Sea transparente y franco en las comunicaciones

Lisa Grigg es la directora del Grupo de Investigación de Fraudes de la División de Delitos Financieros Globales en Bank of America Merrill Lynch. Anteriormente, Grigg cumplió varias funciones en el Bank of America, incluyendo el de oficial de la Ley de Secreto Bancario. Actualmente, es responsable de asegurar el cumplimiento de la Ley de Secreto Bancario y otras leyes federales relacionadas, enmendadas y completadas por las disposiciones pertinentes de la Ley del Patriota de los EE. UU., así como de otras leyes y regulaciones aplicables. Grigg se encuentra muy activa en la Industria. Actualmente se desempeña como co-presidente del Capítulo Carolinas de la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS) e integra el consejo asesor de la 18ª Conferencia Internacional de Antilavado de Dinero y Delitos Financieros de Hollywood, Florida.

ACAMS Today: ¿Podría usted compartir con nosotros algunas ventajas y desventajas que experimentó cuando pasó al sector privado después de su trayectoria como agente de aplicación de la ley?

Lisa Grigg: Mi experiencia anterior como agente de aplicación de la ley me dio una perspectiva única, que me ayudó a comprender de extremo a extremo la aplicación de las leyes y de las regulaciones, a entender la importancia de conocer los hechos, y a tener un enfoque integral de los problemas. Tanto para el sector privado como en el público, sigo pensando que es muy ventajoso tener una red amplia para hacer frente a los problemas que se presentan en la industria.

AT: ¿Tuvo muchas sorpresas cuando empezó a trabajar en el sector privado?

LG: Primero hay que reconocer que cuando entré en el sector privado a finales de los noventas, las cosas eran muy distintas. Sin embargo, lo que me impactó enseguida fue que, en este campo, no hay grandes diferencias entre las misiones de los sectores públicos y privados. En ambos sectores la gente está obligada a hacer lo correcto. Sin embargo el sector público era más fácil conseguir la información necesaria. En el sector privado sólo se ve una pieza del rompecabezas y a veces no se pueden atar cabos. Para los reguladores o para las autoridades de aplicación de la ley, esto es más fácil.

AT: Basándose en su experiencia, ¿hay ideas erróneas en ambos sectores cuando deben tratar entre sí?

LG: El error más común es sobre cómo ve cada parte su papel en el proceso de investigación. El papel del sector privado es el de denunciar las actividades sospechosas, mientras que el papel de los agentes de aplicación es el de investigarlas. A menudo, por cómo ha evolucionado la industria hoy, los agentes de aplicación dependen demasiado de que el sector privado se involucre más en el proceso de investigación, generando una confianza excesiva en esos recursos.

AT: ¿Cuáles son las tres principales lecciones que aprendió sobre cómo pueden mejorar su mutua colaboración las autoridades y los profesionales del sector privado?

LG: A) Comprensión de los roles y de las expectativas, B) El liderazgo de ideas y el intercambio de información son críticos porque están relacionados con un entorno que cambia permanentemente, C) La alianza entre lo público y lo privado es clave para el éxito de la misión en este terreno.

AT: ¿Cuál es la clave para fomentar más cooperación entre las autoridades y las entidades financieras?

LG: En los últimos 10 años, hubo grandes avances en este sentido. La confianza y la comprensión de los objetivos y limitaciones de cada una de las partes es beneficiosa para fomentar el diálogo y abrir canales de comunicación.

AT: Durante la 18ª Conferencia Internacional de Antilavado de Dinero y Delitos Financieros en Hollywood, Florida, el panel "Redefiniendo los Programas de Antilavado de Dinero" abordó el desafío que enfrentan las entidades que reciben mensajes separados por parte de los reguladores y de las autoridades encargadas de aplicar la ley. En su opinión, ¿qué es lo que puede hacer el sector privado, las agencias reguladoras y las autoridades encargadas de aplicar la ley para comunicarse eficazmente?

LG: Ser transparentes y francos en las comunicaciones y comprender que las palabras tienen distintos significados para cada persona, dependiendo de sus experiencias, etc. Complementar el mensaje con un concepto, una explicación o un ejemplo hace una gran diferencia en términos de comprensión y respuesta.

AT: ¿De qué logros en su carrera está más orgullosa, tanto en el sector privado como en el sector público?

LG: Desde ambos lugares, hice mi pequeño aporte para proteger y brindar seguridad a nuestra nación y he ayudado a quitar de las calles a quienes quieren hacer daño.

AT: ¿Qué cualidades busca en un candidato para integrar un equipo de investigación ideal?

LG: Deben ser intuitivos, francos y conocedores de tecnología. Deben tener excelentes habilidades de comunicación (escrita y oral), buen juicio, habilidad para generar redes y, absolutamente, deben ser capaces de aplicar las regulaciones y las leyes a su trabajo diario.

AT: ¿Qué recomendaciones daría sobre cómo tener una carrera exitosa en el actual entorno de Antilavado de Dinero y delitos financieros?

LG: Hay que comprender las aplicaciones de la ley y de las regulaciones para la que uno está trabajando, mantenerse al día en un entorno de amenazas en constante evolución, saber cuándo escalar un asunto y usar buen juicio al tomar decisiones.

AT: ¿Cuáles son las tres cosas que un profesional encargado del cumplimento de la ley siempre debe incorporar a sus políticas de antilavado y programas de procedimiento?

LG:

a. Un Programa de Identificación de Clientes (CIP, por sus siglas en inglés)

b. Diligencia Debida

c. Monitoreo y elevación de informes

Entrevistada por: M. Carolina Rivas, CAMS, principal, Engaged AML Solutions, Inc., Plantation, Florida, EE.UU., carolinarl@engagedaml.com

Consideraciones para la Implementación de un Sistema de Monitoreo Antilavado para las Transacciones Financieras

Las instituciones financieras se encuentran muy dependientes de las tecnologías automatizadas para detectar actividades inusuales o sospechosas. A pesar de que muchas compañías hacen importantes inversiones para implementar y mejorar los sistemas de monitoreo de las transacciones, la necesidad de validarlas — para asegurarse de que son efectivas, exhaustivas y están en consonancia con los riesgos de lavado — sigue siendo un tema común en la aplicación de Acciones de Antilavado de Dinero o ALD.

Desde la perspectiva de la implementación de software, la instalación de un sistema de monitoreo de ALD puede no parecer distinta de la implementación de cualquier otro sistema. Sin embargo, hay factores de riesgo de ALD específicos que toda institución debería considerar. Entre otras consideraciones estándar, quedan incluidos temas como la identificación de escenarios de monitoreo, basándose en los riesgos de actividades sospechosas, en la determinación de los umbrales iniciales para los escenarios identificados y en una metodología sistemática para el ajuste de dichos umbrales. La consideración inadecuada de esos factores podría llevar a mayores costos operacionales, al incumplimiento de los plazos de entrega de los informes, a un alto número de alertas falsamente positivas y, lo más importante, a que se cuelen actividades sospechosas sin detectar, con la consecuente exposición a la crítica por parte de las entidades reguladoras.

A un alto nivel, un enfoque disciplinado para implementar los sistemas de monitoreo de ALD tiene las siguientes ventajas:

- *Escenarios enfocados en el riesgo:* Al ejecutar un proceso sistemático de selección de escenarios, la institución financiera puede seleccionar escenarios específicos adaptando su perfil de riesgo de ALD. La implementación de escenarios de riesgo apropiados puede mejorar la calidad de las alertas y, en consecuencia, la eficiencia del monitoreo y del personal de investigación.
- *Comprensión más profunda de la cobertura del origen de los datos:* A menudo los proyectos de implementación de ALD revelan problemas de arquitectura de datos con sistemas de código o códigos de transacción que deben abordarse como parte del proyecto para asegurar que dentro del sistema de monitoreo ALD ingresen datos adecuados y precisos. Como subproducto de seguir un criterio disciplinado de implementación de sistemas, los implementadores obtendrán un conocimiento profundo de la cobertura de datos (es decir, productos, transacciones, cuentas) relacionados con los escenarios elegidos y, por lo tanto, estarán mejor preparados para responder a las preguntas de los auditores y reguladores, relacionadas con los "metadatos" del sistema de una manera más segura y precisa.
- *Proceso de establecimiento y ajuste del umbral:* Al considerar el establecimiento del umbral como parte integral de la implementación, una institución financiera puede desarrollar un proceso de ajuste sistemático replicable, que le permite adaptar periódicamente los valores del umbral según los escenarios seleccionados de acuerdo con cierto nivel determinado de respuesta a los riesgos (por ejemplo, cambios en la base de clientes, cambios en los productos y servicios, cambios en los comportamientos transaccionales).
- *Proceso eficiente de implementación:* La existencia de una Oficina de Gestión del Proyecto (OGP) promueve una coordinación clara entre los distintos equipos que están a cargo del desarrollo de un sistema de monitoreo libre de problemas. Esta coordinación les permite a los principales interesados obtener una comprensión clara del estado en que se encuentra el proyecto y reaccionar a tiempo para hacer los cambios necesarios.

Consideraciones para la implementación:

Hace falta un esfuerzo importante para lograr un sistema efectivo de ALD de monitoreo de transacciones. Las siguientes son las tareas clave que deberían ejecutarse para implementar con éxito un sistema de monitoreo de transacciones sospechosas de alta tecnología.

1. Planeamiento de los escenarios

En esta fase de la implementación de los sistemas de monitoreo, se seleccionan los escenarios elegibles y las fuentes de datos que proporcionan información para establecerlos. Esta fase incluye las siguientes consideraciones:

Identificación de los escenarios: Esta tarea comprende el mapeo efectivo de los riesgos identificados en la evaluación de riesgos de ALD y las alertas de riesgo ("banderas rojas") más comunes en el lavado de dinero (por ejemplo, las

banderas rojas de lavado de dinero y financiación del terrorismo incluidas en el Manual de Examen del FFIEC BSA/ALD) para las respectivas líneas de negocios actualmente sujetas al monitoreo de transacciones. El mapeo ayuda a identificar las brechas entre los actuales controles de monitoreo y los escenarios necesarios para asegurar una cobertura adecuada de productos/servicios y a mitigar los riesgos de lavado de dinero.

Identificación del origen de los datos: Esta tarea consiste en la identificación de los varios sistemas de origen que albergan los datos requeridos. También incluye la identificación de los procesos que se han de usar para extraer y cargar los datos en el sistema de monitoreo elegido. Los implementadores pueden entonces crear un diccionario (metadatos) de las fuentes de datos y determinar cuáles productos/transacciones deben estar disponibles para el monitoreo. Los siguientes elementos son clave para una adecuada obtención de datos:

- *Disponibilidad de los datos:* ¿Están rápidamente disponibles los datos estudiados?
- *Calidad de los datos:* ¿Se verificó la calidad de los datos? Este es un paso crítico porque la información inexacta (por ejemplo, las transacciones mal codificadas) pueden llevar a análisis sesgados y resultados indeseados o inexactos. Por ejemplo, al diseñar escenarios para capturar comunicaciones enviadas a jurisdicciones de alto riesgo, es imperativo que estén presentes los identificadores de país y que los códigos/valores de país sean exactos.
- *Frecuencia de actualización:* ¿Con qué frecuencia se actualizan los datos?
- *Volumen de los datos:* ¿Se determinó el actual volumen de datos y su potencial escalabilidad? El volumen de datos tiene que poder ser soportado por la actual infraestructura de hardware "tal como está" o bien habrá que identificar recursos de hardware adicionales.

Desarrollo de los escenarios: Esta tarea comprende la traducción de las especificaciones funcionales de cada escenario de monitoreo dentro de un módulo desplegable hecho a la medida del sistema de monitoreo elegido. Generalmente, el proveedor del sistema de monitoreo realiza esta tarea, pero la entidad puede elegir diseñar el código y testear los escenarios por sí misma. Además, la entidad puede desear escenarios personalizados para cubrir adecuadamente sus riesgos de lavado de dinero específicos.

> Es imperativo desarrollar y mantener una documentación apropiada de todos los cambios en los umbrales

2. Determinación del umbral

En esta fase, se identifican los límites para la ejecución de los escenarios identificados. A continuación se enumeran las subtareas clave necesarias para determinar los umbrales iniciales, así como un criterio para la optimización permanente de los escenarios.

Segmentación de clientes: Esta tarea comprende la aplicación de varias técnicas de análisis para los datos en estudio, a fin de determinar la cantidad y el tipo de segmentos de clientes que se pueden desplegar en el sistema. La ejecución exitosa de este paso permite que el equipo implementador pueda determinar los umbrales adecuados para los comportamientos del segmento respectivo, en lugar de usar un único umbral para toda la base de clientes.

Determinación del umbral inicial: En este estadio se aplica un análisis estadístico avanzado para determinar los valores de umbral eficaces para un escenario dado. La determinación del umbral se debe realizar para cada segmento de clientes y nivel de riesgo, lo que significa que puede haber múltiples umbrales para cada escenario.

Ajuste de los umbrales: Antes de aplicar en vivo los umbrales establecidos en la primera determinación, hay que hacer un ensayo para generar alertas que se puedan investigar en un entorno de prueba. La investigación de estas alertas puede clarificar la calidad esperable en el entorno de producción. Esto brinda una buena oportunidad para anticipar ajustes adicionales en el caso de ser necesarios.

Documentación de la metodología de ajuste y su justificación: Es imperativo desarrollar y mantener una documentación apropiada de todos los cambios en los umbrales, incluidos los ajustes finales, para dejar evidencia de la lógica que se empleó y de cómo se ejecutó la metodología definida; y para proporcionar un criterio de base para los ajustes futuros.

3. Despliegue

El despliegue se ejecuta durante todo el ciclo de vida del proyecto e incluye varios tipos de tareas. A continuación, destacamos dos: Examinar y Despliegue de la Producción.

Examinar, examinar y examinar más: El examinar es parte integral de cualquier ciclo de desarrollo de software tradicional, que incluye fases de prueba dedicadas, como el examen de Integración de Sistemas (SIT, por sus siglas en inglés) y el Examen de Aceptación del Usuario (UAT, por sus siglas en inglés). Antes de implementar el sistema de monitoreo en el área de producción, hay que someter las funcionalidades de monitoreo a un examen riguroso de los ciclos SIT y UAT. Los defectos que resulten de ese procedimiento, dependiendo de su severidad, deben ser corregidos o bien agregados al registro de defectos para que así puedan servir como referencia para desarrollos futuros del sistema.

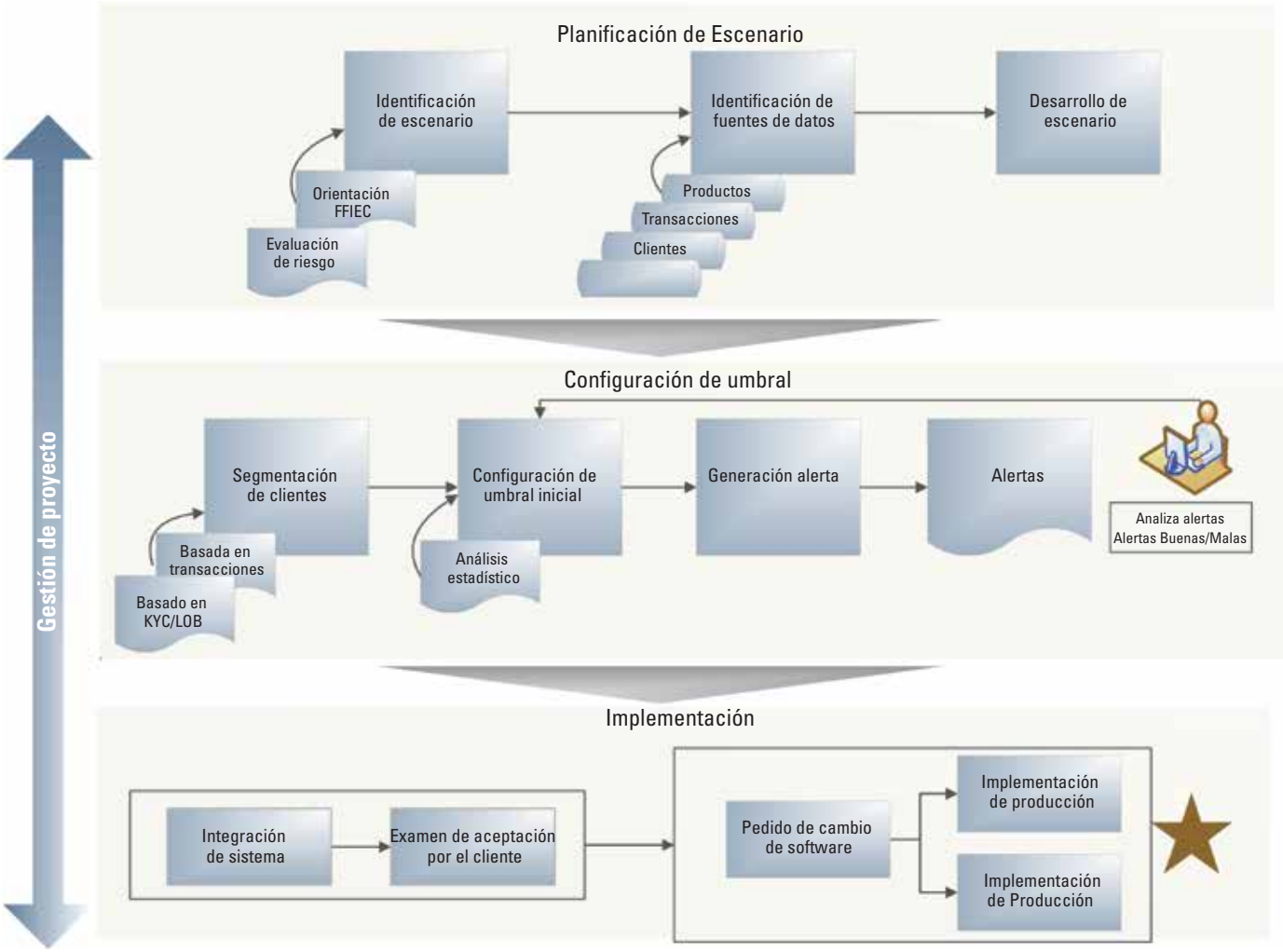
Despliegue de la producción: Después de un ciclo de examinar exitoso, hay que dirigir los componentes del software hacia el entorno de producción. En esta fase, generalmente, se eleva una solicitud de cambio de software a todas las partes interesadas, antes de implementar el software en Producción. Al mismo tiempo, hay que desplegar un software de contingencia para cumplir con los requisitos de recuperación de desastres del sistema.

4. Oficina de Gestión de Proyectos (OGP)

La Gestión de Proyectos es una fase primordial que abarca desde el inicio del proyecto hasta su cierre. La OGP está compuesta por la Planificación del Proyecto, la Gestión de los Recursos y los aspectos de Gestión de los Cambios de la implementación de sistemas.

Planificación de Proyectos: Esta tarea requiere el desarrollo de planes para el proyecto, tomando en cuenta la población, la escasez de recursos y el nivel de esfuerzo requerido para implementar los escenarios elegidos. Si el proyecto se vuelve demasiado complejo debido al código base del software, o a numerosas dependencias, etc., puede ser necesario un plan de desarrollo multifase.

Proceso de Implementación de Monitoreo de Transacciones



Gestión financiera y de otros recursos: Esta tarea implica la comprensión y la gestión eficaz de las limitaciones debidas a las personas y a los recursos del proceso, mediante el desarrollo y seguimiento del presupuesto asignado y a la oportuna elevación de los problemas a los principales actores involucrados.

Gestión de los Cambios: En el transcurso del ciclo de implementación, hay muchos casos que pueden requerir una modificación de los requisitos funcionales, técnicos y de negocios. Para gestionar ese cambio con eficacia y garantizar que se concreten los cambios adecuados en el área de Producción, tiene que haber un proceso de gestión de cambios disciplinado, centrado en la gestión de las solicitudes de cambio, en el pedido de aprobación necesaria de las principales partes interesadas, en mantener un canal de comunicación abierto entre todas las partes responsables y en trabajar con el equipo de implementación tecnológica para poder aplicar eficazmente el sistema en el entorno de Producción.

El cuadro arriba describe un proceso típico de implementación de monitoreo de transacciones.

Resumen

La creación y la ejecución de un plan de implementación de un sistema sistemático de monitoreo de las transacciones, centrado en la identificación del escenario, el origen de los datos, la segmentación de los clientes, el establecimiento de umbrales y los exámenes de funcionalidad permiten a la entidad financiera desarrollar un sistema de monitoreo efectivo, extensible y que satisfaga las necesidades de las principales partes interesadas del negocio y de la tecnología.

Luis Canelon, gerente senior, Protiviti, Consultoría de Riesgo Regulatorio, Londres, Reino Unido, luis.canelon @ protiviti.co.uk

Carl Hatfield, director, Protiviti, Information Technology Consulting, Boston, MA, EE.UU., carl.hatfield @ protiviti.com

Chetan Shah, director asociado, Protiviti, Consultoría Antilavado de dinero, Charlotte, Carolina del Norte, EE.UU., chetan.shah @ protiviti.com

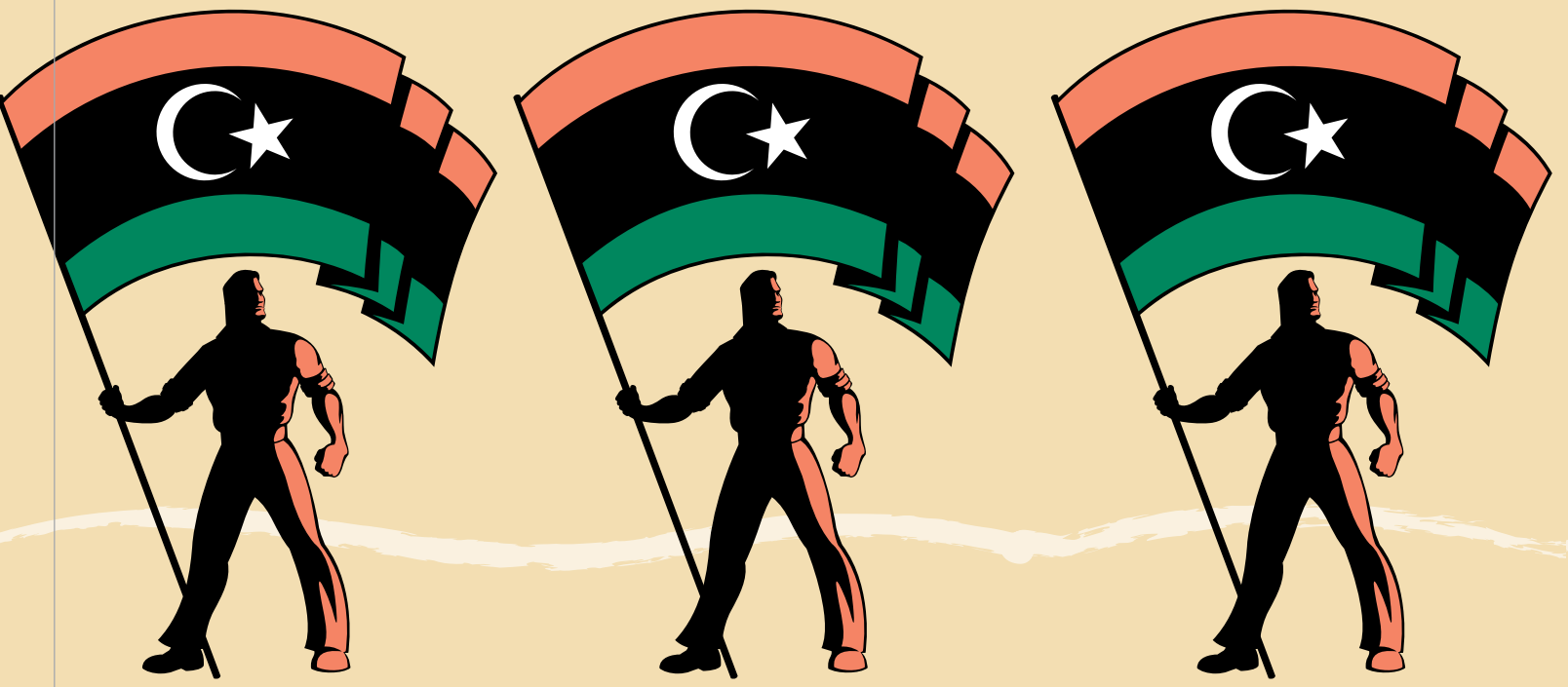
Enfrentarse a las sanciones financieras

—El régimen libio de inmovilización de activos

Las obligaciones impuestas al sector financiero regulado son muchas y variadas, y la mayoría están gobernadas por el enfoque basado en el riesgo, en el que el riesgo de enfrentarse con una persona en particular, empresa o transacción debe evaluarse, y el nivel de debido diligencia por aplicarse debe decidirse sobre la base del resultado de la evaluación de ese riesgo. Esto se aplica en particular a las llamadas Personas Expuestas Políticamente (PEP), individuos de poder e influencia global, tales como políticos y ministros, jueces de tribunales superiores y comandantes militares y de fuerzas de seguridad, etc. La identificación de un cliente en esta categoría debe impulsar el proceso de Debido Diligencia Mejorado y una decisión por parte de la gerencia sobre si se considerará a ese cliente o, en verdad, si se debe hacer un Informe de Actividad Sospechosa (SAR en inglés).

También hay, sin embargo, una clase de individuo o entidad con el cual no se debe tratar bajo ninguna circunstancia, y es esencial que se haga todo esfuerzo de identificar esta clase antes de que las cuentas se aprueben o se empiecen las transacciones. Me refiero, desde luego, a los sujetos de varios regímenes de sanciones globales. Muchos países tienen sus propias listas de individuos sancionados, y les toca a las empresas establecer las maneras de verificar que están al tanto de las listas en los países donde operan, pero por lo más, las listas de la mayor importancia son las operadas por las Naciones Unidas (ONU), la UE, los EE. UU y el Reino Unido. Hay varias listas de la ONU activas, y se pueden encontrar en el sitio web de la ONU.[1] La UE provee una lista comprehensiva que es aplicable a todos los estados miembros,[2] mientras que en los EE. UU., la lista de la Oficina de Control de Activos Extranjeros (OFAC en inglés) cubre empresas con operaciones en los EE. UU. y a cualquiera que trata con dólares

[1] http://www.un.org/en
[2] http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm



estadounidenses.[3] La Tesorería de Su Majestad en el Reino Unido provee una lista comprehensiva que es esencial para empresas británicas, y las empresas que operan en el Reino Unido.[4]

Las resoluciones 1970 (2011) y 1973 (2011) del Consejo de Seguridad de las Naciones Unidas crearon un régimen de sanciones al comienzo del levantamiento popular libio en la primavera de 2011, corregido/ampliado por las resoluciones 2009 (2011), 2016 (2011), 2040 (2012) y 2095 (2013). Las resoluciones originales crearon un embargo de armas, una prohibición de vuelos, la inmovilización de activos y una prohibición de viajes, así como también una Zona de No Vuelo operada por las fuerzas de la OTAN. Las medidas sobre las armas y los vuelos se refirieron a todo el país y población, pero la inmovilización de activos y prohibición de viajar estuvieron y todavía están dirigidas a individuos específicos y a entidades de y controladas por el régimen de Qadhafi. Su propósito era impedir que los fondos fueran usados para seguir reprimiendo y haciéndole daño a la población libia, y obligaba a los Estados miembros a identificar tales activos situados en su territorio, y asegurar que se inmovilizaban y no estuvieran disponibles a los individuos y entidades designados.

El régimen de sanciones de Libia ha sido inusual, en cuanto a que los eventos se desarrollaron muy rápidamente en el verano de 2011, culminando en la caída del régimen y la muerte del líder Coronel Muammar Qadhafi y algunos de sus hijos. En los meses siguientes, las medidas de inmovilización de fuentes fue haciéndose menos estricta para algunas de las entidades, principalmente para ayudar al gobierno de transición y al que con el tiempo llegaría para reconstruir el país. Para mediados de septiembre de 2011, las únicas entidades que quedaban eran y son la Autoridad de Inversión Libia (LIA en inglés), incluyendo la Empresa de Inversión Extranjera Africana de Libia (LAFICO en inglés) y el Portfolio de Inversión Africana de Libia (LAIP). Cualquiera de sus activos que se inmovilizaron o debieron inmovilizarse antes de esa fecha debió permanecer inmovilizado, pero tenía libertad de operar normalmente desde el 16 de septiembre de 2011. El objetivo del Comité de Sanciones de la ONU consiste en levantar la inmovilización de estos fondos tan pronto como una gobernanza financiera estable se logre dentro del país. Los ingresos de la industria petrolera Libia significan que la inmovilización continuada no está afectando la liquidez del país de ningún modo.

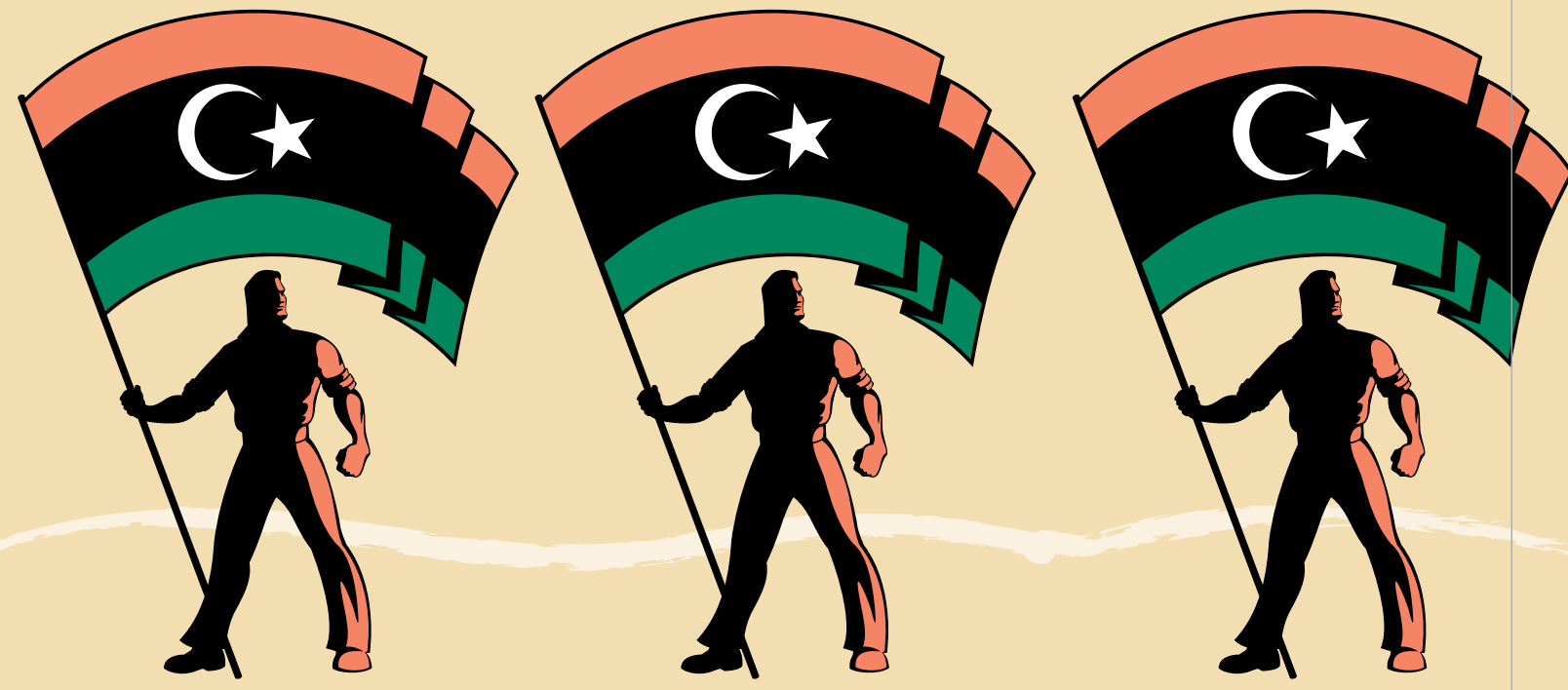
En cuanto a individuos, la inmovilización de fondos sigue siendo total, aun de los fondos de los que han fallecido. Esto es así porque se cree que la mayoría de estos activos fueron obtenidos por miembros del régimen de los cofres del estado, y su inmovilización continuada permite que el nuevo Estado los reclame a través de procesos legales en su día. En verdad, este proceso ya está en curso y el año pasado una corte británica dictaminó que una mansión en Londres, ostensiblemente perteneciente a una empresa registrada en las Islas Vírgenes Británicas, Capitana Seas Ltd., tenía como dueño beneficiario a Saadi Qadhafi, uno de los hijos del ex-líder.[5] La corte le adjudicó la propiedad de $8 millones al gobierno libio.

Todo esto quiere decir que si bien la inversión y el intercambio comercial se encuentran genuinamente alentados con la "nueva" Libia, las instituciones financieras necesitan estar al tanto de la posibilidad que existe de que pueden estar tratando con un individuo designado o asociados, así que tanto su lista de sanciones y sistemas de verificación de dueño beneficiario necesitan ser eficientes cuando contemplan comerciar en la región. Como siempre y en todo lugar, vaya a hacer negocios, pero asegúrese de que ¡Conoce a Su Cliente! A

Simon Dilloway BSC (Hons), MSc, CSyP, FSyl, ex Oficial de la Policía Metropolitana en Londres, director gerente de KYC Cube Ltd y de Lopham Consultancy Ltd, también socio del Panel de Expertos asesores sobre sanciones financieras del Comité de Sanciones de Libia del Consejo de Seguridad de la ONU, Londres, Inglaterra, editor@acams.org

Las opiniones vertidas en este artículo son las del autor y no de ninguna organización de la cual es socio o a la que se encuentra vinculado.

[3] http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx
[4] http://www.hm-treasury.gov.uk/fin_sanctions_index.htm
[5] http://www.reuters.com/article/2012/03/09/us-libya-britain-mansion-idUSBRE82811G20120309



Taiwan: Estudio de caso de un esquema Ponzi y de lavado de dinero por parte de Dream Company

Este artículo se presenta como ejemplo de esfuerzos efectivos de antilavado de dinero en la detección e investigación de cooperación entre los sectores privado y estatales y también como esfuerzo de cooperación importante entre varios gobiernos y departamentos internos. El Sr. Chia-Jui (Mike) Lan, cuyo trabajo de investigación se encuentra en la base de este artículo, es un veterano de larga experiencia de casi 30 años. Se incorporó a la Oficina de Investigación del Ministerio de Justicia como agente especial en 1983, y ha tenido varios cargos de liderazgo en el MJIB (siglas en inglés de la Oficina), incluyendo la de enlace de aplicación de la ley de la Oficina Económica y Cultural de Taipei (Consulado de Taiwán, Vancouver, Canadá), y más recientemente como jefe de sección de la División de ALD. El caso que se comparte aquí es ejemplo de la cooperación necesaria de todos los participantes clave involucrados para traer a la luz la actividad delictiva perpetrada por Dream Company.

Trabajando conjuntamente, los sectores privados y públicos pueden resultar una fuerza efectiva poderosa para detectar y detener el lavado de dinero y el fraude. El estudio de caso que sigue demuestra la efectividad de esta colaboración.

Cómo se detectó al principio

En enero de 2012, el empleado B del banco A entregó un Informe de transacción Sospechosa (STR en inglés) a la división de Antilavado de Dinero (AMLD por sus siglas en inglés). Un resumen del informe dice así: El Sr. W, una persona encargada extranjera, director y gerente general junto con los directores, el senor X y la Srta. Y (la novia del Sr. X) juntamente operaron Dream Company, una empresa incorporada en mayo de 2010. En dos días laborales consecutivos antes de cerrar negocios, las individuos mencionados enviaron al Sr. X y al Sr. Z (el contador de la empresa) a retirar grandes sumas en efectivo del banco A. Sin embargo, no pudieron dar respuestas convincentes a las preguntas del empleado B acerca de la práctica del banco de Debida Diligencia del Cliente (CDD en inglés) respecto del uso de los fondos. El empleado B revisó los antecedentes del cliente, los negocios y transacciones irregulares y sospechó que Dream Company estaba preparando un vaciamiento y que su gerencia escaparía con los fondos. Al empleado B le pareció necesario entregar el STR a la AMLD.

Cómo respondió el FIU

Al recibir el informe, la AMLD empezó a recoger información sobre los antecedentes de la empresa y a analizar las transacciones relevantes. Los investigadores descubrieron que la empresa podría estar usando medios parecidos al esquema Ponzi para defraudar a los inversores. Como resultado, la AMLD refirió el caso a la Oficina Exterior de Taipei, Oficina de Investigación, para que investigara. En febrero de 2012, las autoridades de aplicación de la ley pusieron algunas de las cuentas bancarias de Dream Company en observación como resultado de que un inversor, el Sr. C, se quejara por un impago de Dream Company de la suma principal e intereses que se le debían. Las autoridades también empezaron a investigar a ciertos empleados de Dream Company. El Sr. W fue alertado del hecho y escapó del país el 29 de febrero de 2012. El Sr. X y la Srta. Y trataron de irse del país el 6 de marzo, aunque ya les había indicado el fiscal que no debían ausentarse del país. Fueron arrestados por la Oficina Exterior de Taipei en el Aeropuerto Internacional de Taoyuan. La Oficina Exterior de Taipei inspeccionó las oficinas de Dream Company y a los sospechosos el 7 de marzo.

Durante este período, la AMLD también recibió un STR del personal de cumplimiento de antilavado de dinero del banco A el 7 de marzo de 2012, en el que se decía: "Dream Company depositó 10 millones de dólares taiwaneses en efectivo el 21 de febrero de 2012, pero inmediatamente retiró la misma cantidad el 24 del mismo mes. Su negación a explicar el destino/uso de tal suma incitó al banco a sospechar de blanqueo de dinero, de ahí el informe del banco." La AMLD envió la información para que la investigara la Oficina Exterior de Taipei de la Oficina de Investigación. La AMLD también ayudó a la Oficina a seguir el flujo de fondos de la empresa y a los sospechosos relacionados, como también a la incautación posterior de los fondos.

Los resultados de la investigación

Después de la investigación, se halló que Dream Company había estado involucrada en marketing de varios niveles para defraudar a los inversores. De manera ilícita consiguió de parte de inversores en Taiwán, una suma mayor a 2.5 mil millones dólares de Taiwán (más de 83.30 millones de dólares estadounidenses) supuestamente prometiéndo a los inversores que su

inversión se usaría para instalar sillas de masajes operadas por monedas en supermercados del extranjero y parques temáticos. Los inversores que pagaron ciertas cantidades de dinero, por ejemplo 98,000 dólares taiwaneses (3,500 dólares estadounidenses) o 318,000 dólares taiwaneses (11,000 dólares estadounidenses) por unidad de inversión, recibirían una rentabilidad de 30 por ciento. La empresa insistió en que los inversores recobrarían su principal y más que triplicarían su inversión inicial dentro de 10 meses de inversión. En realidad, la empresa le "robaba a Pedro para pagarle a Paulo" de manera semejante al esquema Ponzi en el que el dinero de inversores siguientes se usaba para pagar la suma principal e intereses de inversores anteriores para defraudar a sus inversores.

En un allanamiento de las oficinas de Dream Company del 7 de marzo de 2012, la Oficina exterior de Taipei de la Oficina de Investigación incautó efectivo que llegaba a aproximadamente 11 millones de dólares taiwaneses (cerca de 400,00 dólares estadounidenses) e inmovilizó fondos bancarios de cerca de 60 millones de dólares taiwaneses (aproximadamente 2 millones de dólares). La AMLD también ayudó a rastrear fondos y al día siguiente (8 de marzo) encontró que hubo flujo ilícito de fondos a las cuentas de los señores W, X, Y y Z. La AMLD luego ayudó a la Oficina Exterior de Taipei de la Oficina de Investigación a inmovilizar los fondos, que eran cerca de 170 millones dólares taiwaneses (aproximadamente 5.50 millones de dólares). Entre agosto de 2010 y febrero de 2012, Dream Company envió más de mil millones de dólares taiwaneses (cerca de 33.30 millones de dólares) de sus ganancias ilícitas a su filial del extranjero. Una suma adicional de 8.40 millones de dólares taiwaneses (cerca de 280,000 dólares) fue enviada a una cuenta bancaria extranjera personal de la Srta. Y.

Resultado de las acciones de la justicia

Los fiscales de la Fiscalía del Distrito de Taipei completaron su investigación en abril de 2012 y pronto iniciaron acciones judiciales en la Corte del Distrito de Taipei. Solicitaron una pena de cárcel de 18 años para el Sr. W, la persona encargada, y para el Sr. X, director de Dream Company; de 16 años para la Srta. Y, otra directora, y de 7 años y 6 meses para el contador de la empresa, el Sr. Z.

Como resultado de que el empleado B del banco A cumpliera diligentemente con los procedimientos de revisión del cliente y Conozca a su Cliente, el empleado estaba familiarizado con el personal y el negocio de Dream Company. Tan pronto como el director y el contador Z intentaron retirar grandes sumas de efectivo, el empleado bancario se dio cuenta de que Dream Company podría estar tratando de concluir su negocio de "inversión" y de cerrar las oficinas. El empleado bancario entonces pudo inmediatamente rellenar un STR. Además, durante la investigación el Banco A hizo que su personal cooperara con la AMLD inmovilizando las ganancias ilícitas en las cuentas pertinentes. Después de las acciones judiciales de las partes pertinentes, la AMLD propuso al banco A que le otorgara incentivos administrativos al empleado B y a otros del personal que ayudaron en confiscar las ganancias ilícitas. La AMLD también había intercambiado información sobre el lavado de dinero mencionado con el centro de inteligencia financiera del país pertinente a través de la red de seguridad del Grupo Egmont. Actualmente la autoridad de aplicación de la ley ha iniciado investigaciones delictivas sobre el Sr. W, quien había huido al país pertinente.

> Los empleados del banco fueron diligentes en su revisión y enviaron pronto un STR

Lecciones claves aprendidas y desafíos

1. Los empleados del banco fueron diligentes en su revisión y enviaron pronto un STR en relación a cualquier transacción sospechosa. También cooperaron con la AMLD (FIU) y las autoridades pertinentes de manera profesional.
2. La AMLD pudo cumplir con su misión llevando a cabo un análisis profundo del STR enviado por las instituciones financieras y lo hizo prontamente enviándolo a las autoridades de aplicación de la ley para mayor investigación. También coordinó el trabajo entre las autoridades locales y la institución financiera, y ayudó a los oficiales de aplicación de la ley durante la investigación para conseguir los informes de transacciones pertinentes y los informes de envíos de divisas de las instituciones financieras y las autoridades financieras supervisoras. Esto ayudó a las autoridades a deducir el flujo de fondos ilícitos en el menor tiempo posible. La AMLD también trabajó con la Fiscalía del distrito de Taipei para inmovilizar e incautar las ganancias ilícitas. No sólo impidió que los sospechosos partieran con los dineros antes de su condena sino que permitió que parte de los fondos fuera devuelta a las víctimas, aminorando las pérdidas.
3. Este es un claro ejemplo de cómo las actividades delictivas pueden enfrentarse cuando hay cooperación total entre las autoridades públicas, las empresas privadas y los centros de inteligencia financiera con una prestación efectiva de la información necesaria y la ayuda profesional de todos los involucrados.
4. Los centros de inteligencia financiera varían de país a país respecto a su naturaleza. También hay disparidad entre los centros respecto de la eficiencia del intercambio de información y su efectividad, de tal suerte que es extremadamente difícil mantenerse al día con la velocidad de la transferencia de fondos a través de las fronteras por parte de los delincuentes. Además, algunos países requieren ejecutar pactos o memorandos de entendimiento con el fin de intercambiar información, de tal suerte que crean ciertas dificultades.
5. También hay muchas limitaciones en relación a la asistencia jurídica. La imposibilidad de extraditar a un sospechoso principal y de obtener pruebas e información de países extranjeros son algunos de los más serios obstáculos para la cooperación judicial.

Taiwán continuará haciendo el esfuerzo de participar en acuerdos o memorandos de cooperación con otros países respecto del intercambio de información. Además, no repararemos en esfuerzos para desarrollar canales oficiales y no oficiales para lograr la cooperación internacional en un nuestra intención de combatir el lavado de dinero transfronterizo.

Enrique Chen, agente especial de la División de Antilavado de Dinero, Ministerio de justicia, Oficina de Investigación, Taiwán, amld@mjib.gov.tw

Revisor Chia-Jui (Mike) Lan, jefe de sección de la División de Antilavado de Dinero, Ministerio de Justicia, Oficina de Investigación, Taiwán, amld@mjib.gov.tw

Contribuidora: Hue Dang, CAMS, Jefe para Asia, ACAMS, hdang@acams.org

Evento del primer aniversario del Capítulo de Hong Kong de ACAMS

El evento del primer aniversario del Capítulo de Hong Kong tuvo lugar en la nueva oficina de KPMG en Causeway Bay Hong Kong el 8 de marzo de 2013 de 5:30 p.m. a 7:30 p.m. Más de 100 socios e invitados participaron en el evento para celebrar el primer aniversario de nuestro capítulo en un viernes soleado y cálido. Participantes de diferentes procedencias con un interés común en el desarrollo de antilavado de dinero en Hong Kong llenaron la moderna sala de conferencia de KPMG para encontrarse con profesionales avezados y así compartir información, establecer contactos y hacer vida social.

Las bebidas y bocados de bienvenida servidos por KPMG constituyeron una manera agradable de darles a los participantes una oportunidad de ponerse al día con viejos amigos y de conocer gente nueva.

Chris Wilson, co-presidente del capítulo de Hong Kong, empezó el evento oficialmente y les dio la bienvenida a los más de 100 participantes. Habló del valor enorme que ha tenido para los profesionales lugareños de prevención del delito financiero que se constituyera el Capítulo de Hong Kong hace un año y la importancia de haber organizado este evento del primer aniversario.

Chris luego introdujo al orador invitado, el Sr. Stewart McGlynn, gerente senior de la Autoridad Monetaria de Hong Kong. Tuvimos el privilegio de tener al Sr. McGlynn como orador invitado con su presentación sobre "Un año de la Ordenanza de Antilavado de Dinero (AMLO) en Hong Kong — Mirando hacia el pasado y el porvenir." Hace un año la nueva legislación de Hong Kong (AMLO) sobre el lavado de dinero y el financiamiento del terrorismo entró en vigencia y el Sr. McGlynn dio un panorama comprehensivo sobre cómo los bancos en Hong Kong se enfrentaron a las obligaciones derivadas de AMLO y los desafíos que ellos y la HKMA enfrentaron el año pasado y a los que se enfrentarían en 2013 y después. La presentación resultó muy informativa y el Sr. McGlynn compartió muchas sugerencias prácticas con el público.

Después de la parte de preguntas y respuestas de la presentación, Kyran McCarthy, el co-presidente del Capítulo de Hong Kong, concluyó el evento agradeciéndole al Sr. McGlynn por su presentación y a todos los participantes por acudir al evento del aniversario.

Para concluir, el evento fue del gusto de muchos y recibimos retroalimentación positiva. La Junta Directiva del Capítulo de Hong Kong querría agradecer a todos los que participaron y ve con beneplácito el hecho de tener más eventos y oportunidades de contacto durante el verano de 2013.

Además del maravilloso evento del primer aniversario, los co-presidentes del Capítulo de Hong Kong dedicaron tiempo a contestar unas cuantas preguntas que les hicieron los socios del capítulo:

¿Cumple con sus objetivos el Capítulo de Hong Kong?

Co-presidentes de HK: El Capítulo de Hong Kong de ACAMS empezó en 2012 — es la misión del capítulo alcanzar excelencia en la prevención del lavado de dinero y el financiamiento del terrorismo, por medio de la creación de un foro en Hong Kong para capacitar e intercambiar ideas dentro de la comunidad de servicios financieros.

¿Cuántos socios del capítulo hay ahora?

HK: El capítulo es uno de los de ACAMS que más rápidamente crece en el mundo y ahora tiene más de 60 socios y sigue creciendo.

¿Qué ha logrado el Capítulo de Hong Kong en el último año?

HK: En el último año el capítulo ha facilitado un número de eventos muy exitosos, que han incluido discusiones sobre tendencias emergentes significativas y desafíos de la comunidad de cumplimiento. El número de participantes en los eventos del capítulo excedió lo esperado — esto es una gran reflexión de la relevancia de las presentaciones y de la calidad de los expertos en los temas.

¿Cuántos y qué tipos de eventos organizó el capítulo el año pasado?

HK: Tuvimos cuatro eventos mayores el año pasado:

- Análisis de la nueva AMLO (marzo 2012): Gavin Shiu — Departamento de Justicia
- FATCA (junio de 2012): Charles Kinsley — KPMG
- Escaneo de pagos de sanciones de próxima generación (diciembre 2012): Jun Claravall
- Citigroup
- Un año de la AMLO en Hong Kong — Mirando hacia el pasado y el porvenir (marzo 2013): Stewart McGlynn — Autoridad Monetaria de Hong Kong

¿Qué metas tiene el capítulo para 2013?

HK: La junta planea por lo menos cuatro eventos claves y reuniones de contacto y haremos circular los detalles de esos eventos dentro de poco. El capítulo también trabajará cerca con ACAMS para identificar beneficios adicionales para los socios del capítulo para incrementar el número total de ellos.

¿Cuáles son las metas de largo alcance para el capítulo?

HK: Nuestra meta de largo alcance consiste en ser una voz significativa en la comunidad de cumplimiento — en particular cuando se necesiten nuevas regulaciones y/o cambios.

Para lograrlo, ampliaremos la membresía más allá de los servicios financieros tradicionales — para incluir otras industrias, profesionales y para respaldar otros capítulos en Asia.

¿Querrían agregar algo más para los socios del capítulo u otros socios potenciales?

HK: El ALD y leyes y regulaciones sancionadoras seguirán creciendo en Asia — esto crea oportunidades significativas y desafíos para los que se encuentran en la comunidad de cumplimiento. Ser socio del Capítulo HK de ACAMS otorga acceso a una red fantástica de profesionales de cumplimiento e instamos a los que no son socios a que se asocien y a los socios a que aprovechen por entero las ventajas de esta red.

Contribuido por el Capítulo de Hong Kong

Sonia Leon
Jefa de Latinoamérica

Sonia León nació y creció en Colombia. Después de estudiar marketing, ingresó en Kraft Foods como supervisora de ventas. Allí estaba a cargo de un robusto grupo de promoción de productos y lideraba la línea de estrategias específicas para el negocio. León se mudó a los Estados Unidos en 2004 y entró en ACAMS ocho años después como ejecutiva de cuentas. Era responsable de acrecentar la cantidad de miembros de ACAMS en Latinoamérica y de desarrollar relaciones sólidas con diversas entidades financieras y gubernamentales, para ayudarlas a cubrir sus necesidades de capacitación en Antilavado de Dinero y prevención de Delitos Financieros. Como resultado de su dedicación y compromiso con los miembros de la región, en 2012, fue promovida a jefa de Latinoamérica. Además, León domina el español, el inglés y el portugués y acaba de completar su programa de MBA en marzo.

ACAMS Today: ¿Podría describirnos su función y sus responsabilidades actuales?

Sonia León: En mi nueva función como jefa de Latinoamérica, estoy a cargo de la dirección estratégica de la región. Estoy liderando los esfuerzos de la compañía para proporcionar beneficios sustanciales a sus miembros, que cubran las necesidades de capacitación de los profesionales a cargo de la detección y prevención de los delitos financieros. También estoy dirigiendo estrategias específicas para cada país, poniendo énfasis en el establecimiento de alianzas a largo plazo con la banca y otras asociaciones profesionales. Dichas alianzas ofrecerán a nuestros miembros amplios recursos, destinados a desarrollar y perfeccionar habilidades para un superior desempeño en el trabajo y un mayor avance en la carrera profesional.

AT: Usted ha estado con ACAMS durante ocho años. ¿Cómo evolucionó la comunidad ACAMS desde que usted empezó a trabajar para la asociación?

SL: Los profesionales que se ocupan de la detección y la prevención de los delitos tienen hoy un trabajo más exigente, por el aumento de las regulaciones y por la transición hacia un sistema financiero más global. Hoy en día, los profesionales tienen más conciencia de la creciente importancia de la capacitación y del desarrollo de las habilidades superiores necesarias para proteger sus instituciones. En el mundo actual, es fundamental mantener programas eficaces de capacitación en metodologías antilavado de dinero y prevención de los delitos financieros.

AT: ¿Cuáles van a ser los temas más candentes en la conferencia latinoamericana de julio?

SL: ACAMS vuelve a Cancún, México, en 2013, para su *7ª Conferencia Anual Latinoamericana sobre ALD y Delitos Financieros.* Este evento es el foro más extensivo de Latinoamérica sobre prevención de delitos financieros. Los profesionales participantes tendrán la oportunidad de interactuar con líderes de la industria en una serie de temas cruciales, tales como:

- Implementación de la Ley de Cumplimiento del Impuesto a las Cuentas Extranjeras (FATCA, por sus siglas en inglés), evitando sanciones.
- Cómo impactan los estándares internacionales y las Leyes Antilavado de Dinero en Latinoamérica.
- Análisis de las últimas tipologías de delitos financieros que afectan a Latinoamérica.
- Ejecución de las recomendaciones recientes del Grupo de Tareas de Acción Financiera (FATF) y análisis de los nuevos criterios de evaluación mutua.
- Aplicación de los procedimientos de Conozca a su Cliente (KYC) y Diligencia Debida Mejorada.
- Aspectos regionales destacados: identificación de tendencias, desafíos y mejores prácticas en el cumplimiento Antilavado de Dinero en la región latinoamericana.
- Cómo los delincuentes integran dólares norteamericanos en países con restricciones al dólar.
- Implementación de un programa anti-soborno y anticorrupción sólido.

AT: ¿Qué obstáculos van a enfrentar los profesionales encargados del cumplimiento de la ley de Latinoamérica en 2013?

SL: Actualmente, las entidades financieras de Latinoamérica están aprendiendo a ser más internacionales y a ofrecer varios servicios financieros globales. Los principales obstáculos que deberán enfrentar los agentes del cumplimiento de la ley son: la construcción de un programa sólido de cumplimiento global, que aborde el aumento de cambios en la legislación y en las regulaciones locales y de los Estados Unidos; alcanzar los niveles esperados por los examinadores — regionales y de los Estados Unidos — y mantenerse al día sobre las últimas tipologías delictivas.

Entrevistada por: Karla Monterrosa-Yancey, CAMS, jefa de redacción, ACAMS, Miami, FL, USA, editor@acams.org

Protect your organization from a world full of risk.

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

Don't blink

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

LexisNexis® understands the nature of risk and delivers AML/compliance, risk mitigation and enhanced due diligence solutions to help you proactively manage it. Solutions such as LexisNexis® Bridger Insight™ XG which now offers unparalleled protection with 100% global sanctions coverage and access to BankersAccuity's Global WatchList® data.

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

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

XCELENT Service 2013

LexisNexis Bridger Insight XG is the winner of Celent's 2013 XCelent Service Award for global watchlists and sanctions.

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

LexisNexis®

Risk Solutions
Financial Services