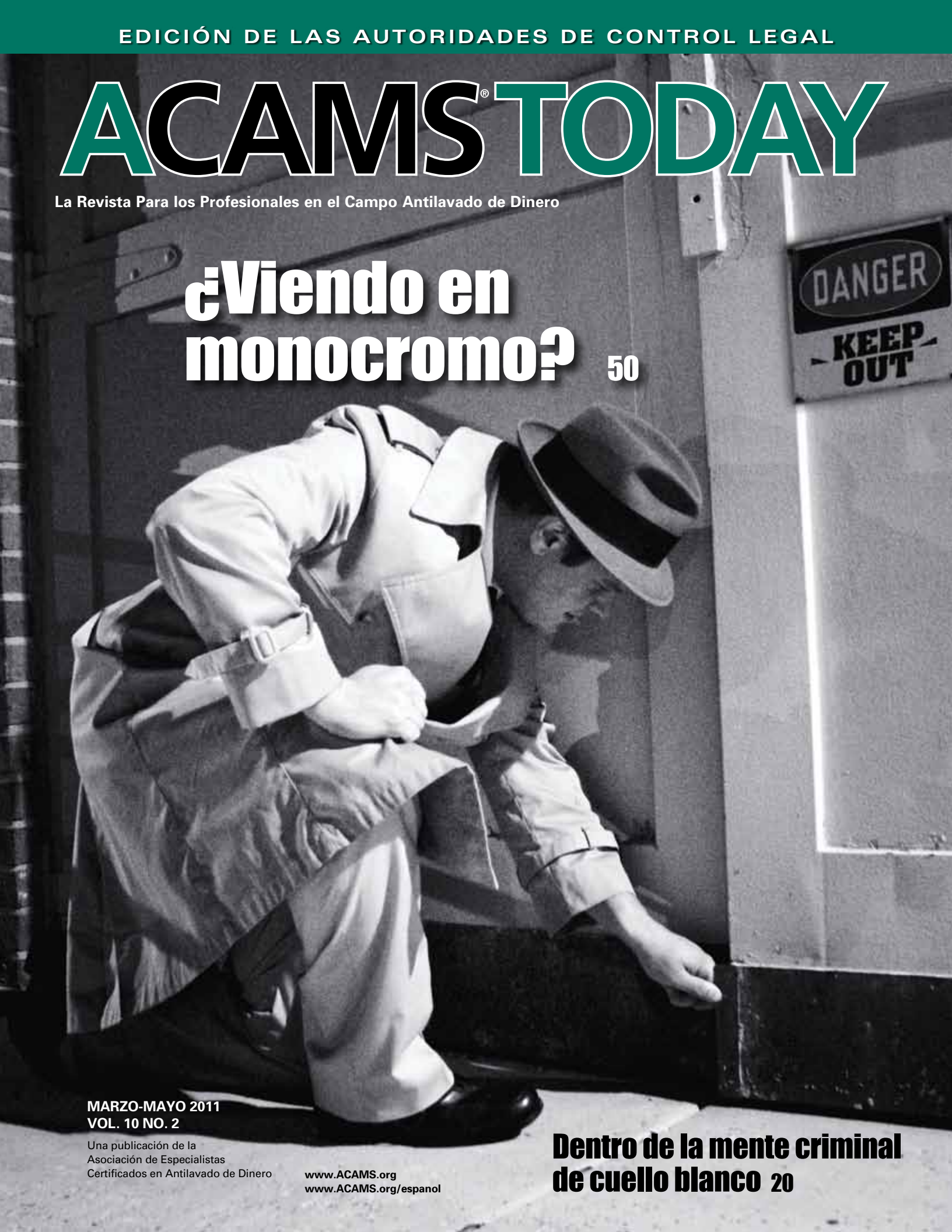
EDICIÓN DE LAS AUTORIDADES DE CONTROL LEGAL

ACAMS® TODAY

La Revista Para los Profesionales en el Campo Antilavado de Dinero

¿Viendo en monocromo? 50



MARZO-MAYO 2011
VOL. 10 NO. 2

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

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

Dentro de la mente criminal de cuello blanco 20

PATRIOT OFFICER®

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

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

Endorsed By The Largest Bankers Associations and Has Passed Examinations

"THOUSANDS OF TIMES"

Financial Intelligence Center

UCEN

Compliance Network UCEN.net

GlobalVision Systems, Inc.

9301 Oakdale Avenue, Suite 100, Chatsworth, CA 91311

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

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

SAS® for Banking

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

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

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

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

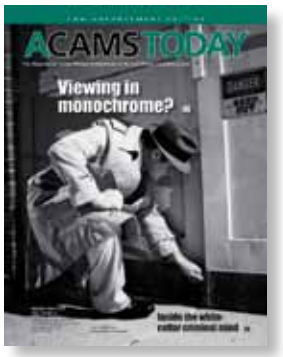
▸▸ **www.sas.com/resilient**
for a free special report

sas | THE POWER TO KNOW.®

Asociación de Especialistas Certificados en Antilavado de Dinero®
ACAMS®

ACAMS TODAY

EN LA PORTADA



Viewing in monochrome?

50

Foto de la portada: Kaitlin Racine

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

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

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

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

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

EN ESTA EDICIÓN

DE LA EDITORA

Algunos de mis programas favoritos de TV incluyen a policías, detectives e investigadores. Últimamente, estuve mirando *Hawaii Five-O*, *Castle*, *White Collar* y *el Mentalista*. Siempre me pregunto qué hace que los programas sobre policías y detectives sean tan atractivos para la sociedad en general. Para la gran mayoría de la gente, lo más cerca que llegan a estar de interactuar directamente o cruzarse con un oficial de control legal es el jueves a la noche en el sofá viendo su programa favorito de policías. Sin embargo, para aquellos en el campo ALD que interactúan con las autoridades de control legal es parte de la rutina. Hemos creado esta edición especial de *ACAMS Today* para destacar los esfuerzos conjuntos de ambos profesionales, con el objetivo de ayudar a los profesionales de cumplimiento y a los profesionales de control legal a formar asociaciones exitosas.

El artículo principal *¿Viendo en monocromo?* Analiza la importancia de conocer las distintas perspectivas entre el cumplimiento y el control legal. Conozca la importancia del trabajo en conjunto y cómo pueden las innovaciones apoyar los esfuerzos de los profesionales de cumplimiento y de control legal a combatir el crimen.

¿Alguna vez se preguntó qué sucede dentro de una mente criminal? *Adentro de la mente criminal de cuello blanco* brinda una rápida mirada al enigmático mundo de un criminal. Descubra las cualidades inmorales que pueden ayudarle a descubrir a un criminal de cuello blanco dentro de su organización.

Constantemente tomamos decisiones todos los días de nuestra vida. El artículo *Cuándo llamar a las autoridades de control legal* ofrece guías sobre cómo toma la decisión correcta. Conozca qué tienen que decir los expertos sobre cuándo debería hacer esa llamada importante.

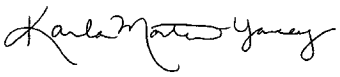
Los criminales tratan constantemente de explotar todos los ángulos. El artículo *Crimen organizado a su paso* reseña cuáles son las cuatro áreas que toda institución debería tener en cuenta. Los criminales dependen de su conocimiento de la naturaleza humana cuando tratan de aprovecharse de su institución.

Determine la importancia de la calidad del reporte en *Reporte de Actividad Sospechosa: Asegurar la calidad es fundamental para maximizar el valor del reporte. El artículo reseña cómo obtener ROSs de calidad siguiendo las cinco "W's"*. Recuerde que los ROS redactados incorrectamente podrían impactar negativamente en los esfuerzos del control legal en una investigación.

Como profesionales ALD nunca podemos decir "Regístrenlo y tómenle las huellas digitales" ("Book 'em Danno") pero trabajar de cerca con las autoridades de control legal nos ayudará a todos a contribuir a minimizar el crimen.

Además, quisiéramos agradecer a nuestros muchos autores que colaboran con *ACAMS Today* y por ello quisiéramos que ustedes, los lectores, nominen a un artículo de 2010 que hayan disfrutado o hayan considerado el más útil para el *Premio al Artículo del Año de ACAMS Today*. Por favor indiquen el título del artículo, autor, en qué edición fue publicado y un breve resumen para fundamentar su nominación. Todas las nominaciones deben recibirse hasta el 1 de Agosto de 2011. El ganador recibirá su premio en la Conferencia Anual de ACAMS en Las Vegas, Nevada en Septiembre.

Como siempre, no se olviden de enviar sus comentarios e ideas para los artículos, remitiendo la presentaciones directamente a mí a editor@acams.org.



Karla Monterrosa-Yancey, CAMS
editora/gerente de comunicaciones
ACAMS

Noviembre–Enero Graduados CAMS

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

GRADUADOS CAMS

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

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

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

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

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

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

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

El señor Rajwani actualmente es el oficial jefe antilavado de dinero del RBC Financial Group (RBC). Él es responsable de la dirección del programa ALD Global del RBC, que abarca iniciativas sobre antilavado de dinero, antiterrorismo, sanciones económicas, antisobornos, anticorrupción, administración de riesgo de clientes. Basándose en más de 20 años de experiencia en administración del riesgo, cumplimiento y contabilidad financiera, Rajwani es una autoridad líder en temas antilavado de dinero y contra el financiamiento del terrorismo tanto a nivel local como internacional y frecuentemente realiza presentaciones sobre estos temas en plataformas bancarias, legales, de cumplimiento y académicas.

Rajwani es copresidente del Capítulo de Canadá de ACAMS y también es miembro designado del Consejo Asesor sobre Seguridad Nacional de la Oficina del Primer Ministro de Canadá sobre temas de seguridad nacional.

Rajwani ha supervisado el desarrollo e implementación del programa CFT/ALD de RBC desde su concepción. Como oficial jefe antilavado de dinero del banco más grande de Canadá, Rajwani ha dirigido el desarrollo e implementación de varias soluciones ALD en el RBC que abarcaban a oficinas en 53 países y clientes de las plataformas de banca minorista, administración de bienes, seguros, corporaciones y banca de inversión.

Antes de asumir su cargo actual en el RBC, Rajwani ejerció varios cargos gerenciales cuya tarea principal estaba centrada en la administración de riesgo, controles internos, riesgo operativo y desarrollo IT. Además de su experiencia en administración del riesgo, Rajwani ha trabajado para varias Instituciones Financieras, firmas Consultoras Colegidas de Contabilidad y Administración supervisando la implementación de las iniciativas de administración del riesgo y cumplimiento a nivel general de la empresa.

Rajwani ha obtenido con honores dos títulos en Contabilidad y Financias y es miembro del Instituto de Contadores Colegiados de Canadá, Inglaterra y Gales.

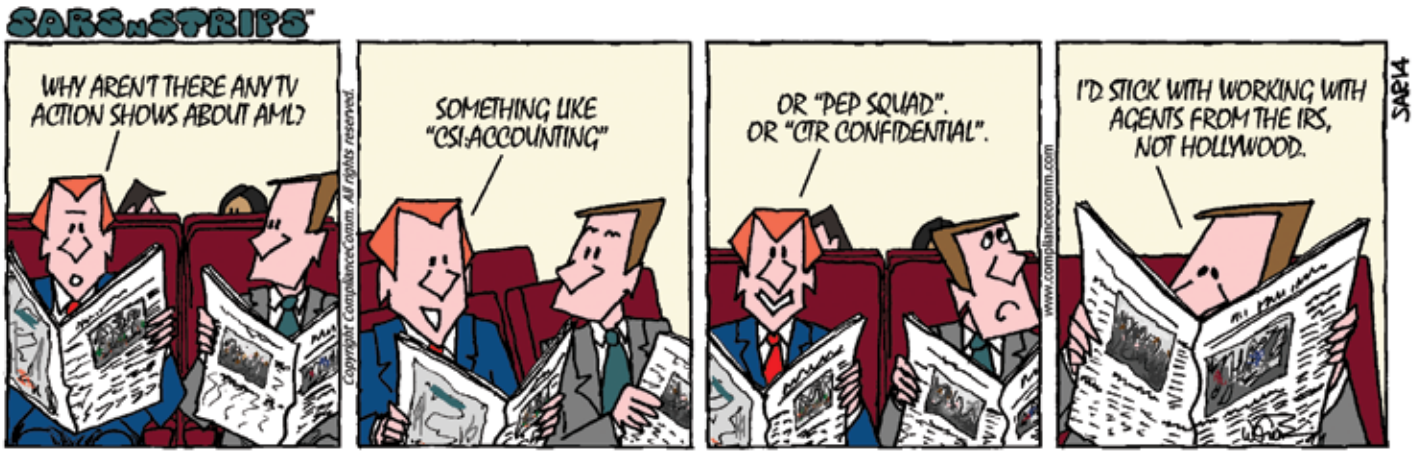
David M. Schiffer
Mineola, New York

David Schiffer es el fundador y presidente de Safe Banking Systems (SBS), firma proveedora de soluciones ALD y de cumplimiento con oficinas centrales en Mineola, NY. Durante más de una década, Schiffer ha dirigido los esfuerzos de su compañía para combatir el lavado de dinero, financiamiento del terrorismo, fraude y otras actividades criminales ofreciendo a las bancos, instituciones financieras no bancarias y corporaciones, la última tecnología para combatir el crimen financiero y encontrar a los "malos".

El apoyo de Schiffer a ACAMS data desde su creación cuando Safe Banking Systems se convirtió en el primer miembro de servicios de ACAMS. Su hijo Mark, un ejecutivo de la compañía, obtuvo la designación CAMS como integrante de la primera promoción de miembros en ser certificados. SBS está orgullosa de su historia con la organización ACAMS como auspiciante de eventos y colaborador en ACAMS Today. Schiffer ha escrito dos artículos, "El Desafío de las PEPs" y "Riesgo generado internamente".

Schiffer considera que el rol de SBS no es solo proveer soluciones innovadoras a los clientes sino también compartir conocimientos prácticos y experiencias. Se ha reunido con asesores legales jefe y sus equipos de investigación tanto en el Comité de Comercio del Senado de los EE.UU. y con el Comité sobre Seguridad Interior de la Cámara de Representantes del Congreso de los EE.UU., y ha sido entrevistado por varias radios.

Antes de fundar SBS, Schiffer dirigió otras compañías tecnológicas y también enseñó en el sistema escolar de la ciudad de Nueva York. Como oriundo de la ciudad de Nueva York, Schiffer obtuvo su título de Maestro en Ciencias en Ciencia de la Computación en SUNY Stony Brook, su Maestría en Artes en Matemática en el Colegio Hunter, NY y se graduó como Bachiller en Ciencias en Matemáticas también en el SUNY Stony Brook, NY. En Agosto de 2010, Schiffer fue premiado por la Fundación Estadounidense del Riñón por su apoyo benéfico a su entidad.



Producido por ComplianceComm

Una manera estupenda de estar conectados

Estamos muy orgullosos de publicar esta "Edición Especial de Control Legal" de *ACAMS Today*. Sé que la van a encontrar tan valiosa como yo, concentrada totalmente en los hombres y mujeres de control legal, que la primera línea de la comunidad contra los criminales de todo el mundo.

Cuando me uní a ACAMS en febrero pasado, me comprometía reconocer el rol importante que el control legal tiene en nuestra organización y en los esfuerzos globales para combatir el lavado de dinero, el crimen financiero y todos los demás esfuerzos relacionados que tienen un componente monetario. El año pasado, me reuní con representantes de control legal estatales, federales e internacionales para analizar cómo mejorar nuestra capacitación, y la concientización general de toda la comunidad ALD global. Seguramente veremos más capacitación de ACAMS sobre investigaciones, respondiendo a solicitudes de información de control legal y cómo preparar RASs o ROSs. Las agencias de control legal son verdaderos socios del sector privado profesional ALD y necesitamos hacer nuestra parte para ayudarles.

Por favor háganos llegar sus comentarios sobre este esfuerzo e ideas para temas para futuras ediciones.

Capítulos de ACAMS — Una excelente manera de estar conectados

Tuvimos un 50 por ciento de incremento en los capítulos de ACAMS en 2010. Tenemos nuevos capítulos en Florida, el medio oeste, noreste y la costa oeste de los Estados Unidos, También se crearán capítulos en Europa, Asia, América Latina y el Medio Oriente. Durante 2011 seguirán creciendo, y con las recomendaciones elaboradas por el Comité Directivo creado en diciembre, los capítulos serán realmente una manera importante mediante la cual nuestros miembros puedan estar vinculados entre sí.

Tuve la suerte de poder viajar a las inauguraciones de varios capítulos y estoy realmente muy impresionado por el profesionalismo mostrado por los miembros de las juntas. Su compromiso para alentar la participación y propuestas asegurará que los miembros de ACAMS se mantengan activos y conectados en el futuro.

Es fundamental que las juntas de nuestros capítulos estén compuestas por una amplia variedad de profesionales ALD de los sectores del gobierno, consultoría y la industria financiera. Hay que tener presente en el momento de la creación de un capítulo en su área, que cuanta mayor diversidad exista en su junta directiva, mayor valor podrá brindársele a los miembros locales de ACAMS.

El Examen CAMS — Una evaluación del profesional ALD como ninguna otra

Otra área de fundamental importancia para los empleadores tanto del sector público como privado es si un postulante profesional ALD está realmente preparado para los desafíos de esta industria. Tuve la suerte de haber estado en esta comunidad durante mucho tiempo (por favor, ¡no se rían!) y para mí está claro que el examen CAMS es la única verdadera medida de evaluación del conocimiento ALD. No existe una competencia válida para nuestro proceso y acabamos de actualizar el examen en 2011 para reflejar los cambios en las leyes, regulaciones y cobertura relacionada con el ALD. Nuestro examen también es analizado psicométricamente y no es un examen "a libro abierto". ¡Tampoco "apadrinamos" a nadie! Por ello, la próxima vez que lo contacte la competencia, recuerde, no hay competencia. Enorgullézcase de su designación CAMS y comparta historias con nosotros sobre cómo esa credencial le ha ayudado en su carrera.

Actividad de los Grupos de Trabajo — Otro vehículo de participación

ACAMS ha tomado la decisión estratégica de revisar todos nuestros grupos de trabajo actuales y crear varios grupos nuevos. Creemos firmemente que la ampliación de los grupos de trabajo, los capítulos y otros comités crearán grandes oportunidades para que los miembros participen en la comunidad de ACAMS.

En algunos casos, los miembros de ACAMS que han participado durante mucho tiempo destacándose, ya no forman parte de varios de nuestros grupos de trabajo y hemos incorporado miembros o individuos nuevos que han sido miembros pero que nunca han participado en un rol activo. Este enfoque puede parecer severo, pero no debería considerárselo de esa manera.

Para poder planificar las conferencias y tener asesoramiento sobre la capacitación, es importante que ACAMS conozca a los nuevos miembros de nuestra diversa comunidad — sea que se trate de NSMs, seguros, valores, casinos u otros de la comunidad de consultoría ALD. Creemos que estos cambios traerán beneficios inmediatos.

Estoy convencido que los dedicados miembros de ACAMS encontrarán la manera de participar y le damos la bienvenida a ese apoyo.

Para comenzar a pensar sobre su nueva participación o sobre cómo modificar su actuación ya en curso, por favor cuéntenos sobre su interés en cualquiera de los siguientes grupos de trabajo:

- Sanciones
- Tráfico de Personas
- Títulos valores
- Seguros
- Unidades de Inteligencia Financiera (UIFs)
- América Latina
- Caribe

Finalmente, por favor le agradeceremos su comentario sobre si tiene alguna sugerencia para algún otro grupo de trabajo.

John J. Byrne, CAMS
ACAMS vicepresidente ejecutivo

Simon Dilloway: Siga el rastro del dinero

ACAMS Today tuvo la oportunidad de conversar con Simon Dilloway, fundador de Lopham Consultancy.

Dilloway trabajó más de 30 años en la Policía Metropolitana en Londres. Se especializó en la investigación de la corrupción, delitos financieros y financiamiento del terrorismo mediante el uso de métodos de investigaciones financieras y la obtención y análisis de información financiera. Mientras dirigía un equipo en la Unidad Nacional de Investigaciones sobre Financiamiento del Terrorismo de la Oficina Especial de la Nueva Scotland Yard (NTFIU, por sus siglas en inglés), utilizó estas técnicas con gran resultado luego de los ataques con bombas perpetrados en Londres en 2005. Posteriormente dirigió la operación de investigación financiera y obtención de información que llevó al arresto y condena de los terroristas que participaron en la conspiración para derribar siete aviones que se dirigían a América del Norte. Desde su retiro de la policía y creación de Lopham Consultancy, colaboró con la Comisión Europea, el Consejo de Europa y la Oficina de las Naciones Unidas sobre Narcóticos & Delitos en la preparación de misiones en todo el mundo. Las capacitaciones dadas por él sobre ALD y en particular sobre CFT han sido bien recibidas por el personal de control legal de Rusia, los Balcanes, el Medio Oriente (incluido Irak) y el norte de África, así también como del Reino Unido, donde es un entrenado asociado sobre crimen financiero de la NPIA. Ha realizado exposiciones en varias conferencias internacionales, y recientemente hizo una presentación sobre financiamiento del terrorismo en el Comité del Grupo de Trabajo de la OTAN en Bruselas, Actualmente está abocado a la nueva redacción de los manuales nacionales de investigaciones y procesos judiciales antilavado de dinero de la República de Vietnam.

Tiene el título de Bachiller en Ciencias (con honores) en Estudios Policiales, y una Maestría en Ciencias en Justicia Criminal. Es miembro de ACAMS, el Instituto de Directores y Director & Miembro del Instituto de Seguridad del Reino Unido.

ACAMS Today: ¿Puede describir su cargo y responsabilidades actuales?

Simon Dilloway: Tengo mi propio negocio que incluye a varias compañías. Mi trabajo principal en este momento es la capacitación ALD y el asesoramiento al sector público/de control legal internacional. Además, acabo de regresar de realizar visitas de capacitación en Rusia y Ucrania, y estoy en el medio del proceso de reformulación del Manual Vietnamita para los investigadores de LD y fiscales. Además, realizo análisis y soluciones ALD a empresas reguladas del Reino Unido, y tengo un tercer interés en un sitio de aprendizaje en línea y verificación de nombres que actualmente está en preparación.

AT: ¿Cómo empezó a actuar en el control legal y el campo del cumplimiento?

SD: Ingresé a la Policía Metropolitana en Londres en 1976, y trabajé allí durante casi 31 años. La última parte de mi trabajo allí fue como detective investigador financiero, trabajando con temas de anticorrupción,

tráfico de drogas, lavado de dinero y finalmente, terrorismo en la Unidad Nacional de Investigaciones de Financiamiento del Terrorismo (NTFIU), que por entonces formaba parte de la Oficina Especial en la Nueva Scotland Yard. Luego de mi retiro en 2007, inicié las compañías mencionadas anteriormente, y empecé mi nueva carrera en el campo del cumplimiento.

AT: ¿Cuál es la clave para tener una relación laboral exitosa entre las autoridades de control legal y los profesionales de cumplimiento?

SD: Esto es algo en lo que participaba mucho cuando estaba en la NTFIU. La principal relación tiene que ser de confianza mutua — esto es lo más importante. Claramente, aquellos que actúan en el cumplimiento tienen obligaciones legales, tanto en lo que se refiere a divulgación como a confidencialidad, y por el otro lado, el control legal tiene que tener cuidado de no revelar información sensible o clasificada. Si, sin embargo, ambos sectores pueden ir más allá para facilitar el trabajo de cada uno, estaremos un paso más cerca de ganarles a los malos.

AT: Durante su carrera participó de varias investigaciones ALD, de financiamiento del terrorismo y de delitos financieros, ¿qué elementos en común encontró en ellas?

SD: ¡Es una pregunta interesante! Paradójicamente, una de las cosas en común es lo diferente que es cada investigación. Con ello quiero decir que cada vez que se investiga sobre lavado de dinero o terrorismo, se encuentra un nuevo elemento que no había visto antes, porque los criminales siempre están desarrollando métodos nuevos ante las mejoras legislativas constantes. Por esto es que siempre predico tan apasionadamente sobre el enfoque basado en el riesgo. Es la única manera de evitar quedar empantanado en crear tipologías, lo que en sí mismo lleva a no detectar los métodos nuevos para transferir u ocultar el dinero sucio.

AT: ¿Cómo pueden esos elementos en común ser utilizados mejor por el profesional e cumplimiento?

SD: Los elementos comunes que existen tienen que ser compartidos. Éste es un área donde la competencia debe ser dejada de lado, y las experiencias de una institución deberían ser difundidas a todos. Esto por supuesto es promovido por muchas organizaciones de la industria — especialmente ACAMS. Idealmente, las empresas deberían estar en posición de utilizar sus conocimientos ALD como una herramienta de marketing, indicándole a los criminales, clientes y la industria que son un objetivo difícil. Además, un régimen ALD bien dirigido también mantiene un control más estricto sobre otros sistemas en la empresa, mejorando de esta manera la dirección en general.

> Los criminales siempre están desarrollando métodos nuevos ante las mejoras legislativas constantes

AT: ¿Qué indicadores de financiamiento del terrorismo (FT) deberían buscar las instituciones y qué consejo daría sobre cómo pueden protegerse las instituciones contra el FT?

SD: Como señalé en artículos anteriores, la naturaleza de la mayoría del FT es tal que es muy difícil de detectar. Las finanzas de quienes atacaron con bombas en Londres, en retrospectiva, indicaban claramente qué estaban haciendo y porqué; sin embargo, eso fue solo con el conocimiento de que lo hicieron después. La situación real no era diferente de la de muchos otros jóvenes del mismo grupo étnico. Las instituciones deberían buscar transacciones hacia o desde países conocidos por destinos, o puntos de tránsito de FT. Deberían verificar detalladamente la identidad de los clientes, y estar especialmente atentas antes cualquier reticencia a dar evidencia respaldatoria de la identidad.

En realidad, sin embargo, no existe un método infalible más allá de lo que se hace para el ALD. Lo importante es asegurar que los procedimientos sean tan estrictos como sea posible, y que la conservación y archivo de los registros sea precisa y eficiente, para que cuando las autoridades de control legal entren en contacto con las instituciones, las empresas puedan entregar rápidamente información de primera calidad. Esa es la mejor ayuda que puedo recibir como investigador.

AT: ¿Cómo ayuda el seguimiento del rastro del dinero para iniciar un caso ALD o de FT?

SD: Poder conectar al delito con los fondos es el objetivo final del investigador ALD. El propósito general de la actividad del lavador es ocultar el dinero a través de complejos estratos de transacciones y transferencias, y proteger el botín para utilizarlo después — como sabemos. Si se puede seguir el rastro del dinero con pruebas, no solo se puede identificar dónde está, sino que se tiene la posibilidad de confiscarlo. Además, cuando todos los detalles misteriosos y bizarros de las distintas etapas del ocultamente son presentados ante un tribunal como evidencia, en realidad fortalece el caso y ¡muestra al lavador claramente como el delincuente!

AT: ¿Cuál es trabajo sobre lavado de dinero o financiamiento del terrorismo del que más se enorgullece?

SD: Además de preparar el doloroso y costoso informe por los ataques con bombas producidos en Londres en julio de 2005, de lo que estoy más orgulloso es de dirigir la investigación financiera del plan para hacer estallar los aviones que se dirigían de Londres a América del Norte. Lo que empezó como una pequeña investigación de FT hasta que me retirara de la policía se convirtió en la investigación de la mayor amenaza terrorista que enfrentó el Reino Unido. Si esos ataques se hubieran llevado a cabo con éxito, podrían haber perdido sus vidas unas 4.000 personas, y estoy inmensamente orgulloso de haber sido parte de la operación que impidió que eso sucediera. También significa que ahora va a tener problemas en llevar su pasta dental en el vuelo, ¡por lo que le pido disculpas por los inconvenientes!

Entrevista realizada por Karla Monterrosa-Yancey, CAMS, editora, ACAMS, editor@acams.org

David Olesky:

Mejores líneas de comunicación produce mejores resultados

A *CAMS Today* se reunió con el Agente Especial David Olesky en una entrevista informativa. El Agente Especial Olesky ha trabajado en la Administración de Control de Narcóticos (*Drug Enforcement Administration*, o DEA, por sus siglas en inglés) durante más de diez años. Se ha desempeñado en la División de Nueva Jersey de la DEA y en la Oficina de la DEA en Panamá. Antes de ingresar a la DEA, GS Olesky trabajó varios años como auditor de una firma contable donde obtuvo su licencia de contador público certificado.

ACAMS Today: ¿Puede describir su cargo y responsabilidades actuales?

David Olesky: Soy Supervisor del Grupo de Agentes Especiales del Grupo de Investigaciones Financieras de la DEA en Los Ángeles. Nuestro grupo se concentra en los traficantes de drogas más importantes que operan en el sudoeste de los Estados Unidos que están lavando el dinero tanto dentro como fuera del sistema financiero.

AT: ¿Cómo empezó a actuar en el control legal y el cumplimiento?

DO: Antes de ingresar a la DEA, había trabajado varios anos para una firma contable pública, había obtenido mi licencia de CPA, y poco después me postulé para la DEA. He trabajado en la DEA más de diez años, y con mis antecedentes en contabilidad, fue casi un hecho natural que eventualmente me encontrara en el Grupo de Investigaciones Financieras. El año pasado, interactué más con oficiales de cumplimiento como resultado de las oportunidades de contactos con colegas que se presentaron a través de ACAMS. Mi grupo tiene mucha interacción con las instituciones financieras en razón de la naturaleza de la misión de nuestro grupo.

AT: ¿Cómo pueden los profesionales de cumplimiento trabajar más eficientemente con las autoridades de control legal?

DO: No teniendo miedo de hacer preguntas e interactuar con los agentes y funcionarios. Cuando su oficial de cumplimiento recibe una solicitud judicial de las autoridades de control legal, puede contactar sin ningún problema al agente y analizar el pedido. Por supuesto que los investigadores no pueden divulgar nada que potencialmente pudieran comprometer a la investigación; sin embargo, hay un nivel medio práctico donde tanto el investigador como el oficial de cumplimiento pueden trabajar óptimamente. Las investigaciones de lavado de dinero tienden a ser complejas, llevan mucho tiempo y pueden incluso durar varios meses — sino años. Es mejor si ambos lados pueden establecer una relación profesional para que tanto el investigador como el oficial de cumplimiento entiendan los objetivos. Para un agente de la DEA, incluso para mí por haber trabajado en el sector financiero, puede ser muy intimidatorio aceptar hacerse cargo de una investigación financiera. La mayoría de los agentes están más cómodos tirando abajo la puerta de alguien en el medio de la noche que reuniéndose con un oficial de cumplimiento para analizar registros financieros. Como resultado de ello, cuando mejor sean las líneas de comunicación entre los dos sectores, también serán mejores los resultados.

AT: Como profesional del control legal, ¿cuáles son los tres elementos más importantes que usted busca en una investigación de lavado de dinero?

DO: Número 1, buscamos cómo el sujeto objeto de la investigación ingresa primero sus fondos procedentes de la droga en el sistema financiero. La identificación de la relación entre la actividad ilegal específica (SUA, por sus siglas en inglés) y la entrada del dinero en el sistema financiero es fundamental. Por esto es que conocer a su cliente (CSC) es muy útil para la comunidad de control legal. Para nosotros es fundamental identificar el quién y cómo es sujeto comienza a ingresar los fondos dentro del sistema. Número 2, tratamos de ampliar nuestra investigación al máximo para identificar a todas las cuentas, bienes e individuos asociados. Y Número 3, tratamos de rastrear el flujo del dinero una vez que ingresa en el sistema esperando identificar los elementos adicionales en la conspiración y también en los posibles decomisos como conclusión de la investigación.

AT: ¿Cómo pueden los colegas del sector de control legal prepararse para trabajar de manera efectiva con las instituciones financieras (IFs) en una investigación?

DO: Teniendo una estrategia y siendo específico en sus pedidos a las instituciones financieras. Allí es donde nuevamente, las líneas de comunicación entre las dos partes es vital.

AT: ¿Cuáles son los últimos esquemas que ha visto en las investigaciones de lavado de dinero y cómo pueden prepararse las IFs para combatir estos esquemas?

DO: En junio de 2010, el ministerio de finanzas mexicano publicó regulaciones nuevas que restringen las transacciones en efectivo en dólares en los bancos mexicanos. La regla prohíbe a los bancos recibir dólares en efectivo para transacciones como cambios de monedas, depósitos, pagos de préstamos, o compras de servicios, incluidas las transferencias de fondos, excepto cuando esas transacciones son realizadas bajo ciertos montos máximos. Para los individuos que son

clientes, el límite total en dólares en efectivo que el banco puede recibir de su cliente por mes calendario es de solo US$ 4.000. Creo que estas restricciones tendrán un impacto en el flujo de los fondos ilegales provenientes del tráfico de drogas (dólares en efectivo). Esto seguirá siendo un mercado subterráneo en México, donde la moneda estadounidense es movilizada fácilmente; sin embargo, creo que veremos más dólares en efectivo permaneciendo dentro de nuestras fronteras e ingresando al sistema financiero cuando antes eso hubiera ocurrido al sur de nuestras fronteras. La información preliminar que he visto en los últimos meses ha reflejado eso. También escuché informes sobre un incremento en las cuentas bancarias de clientes a lo largo de la frontera entre Estados Unidos y México, esto puede atribuirse a este cambio en las regulaciones.

AT: ¿Puede comentar información general sobre los últimos casos en los que está trabajando?

DO: Nuestro grupo tiende a concentrarse en los carteles mexicanos de drogas y en los componentes financieros asociados con el tráfico de drogas que realizan. Estos grupos son muy astutos, y utilizan una amplia variedad de métodos para movilizar su dinero — desde el clásico transporte de grandes cantidades de dinero en efectivo a través de la frontera para su utilización en el Mercado Negro de Cambio de Pesos (*Black Market Peso Exchange*, o BMPE por sus siglas en inglés). Con el cambio en las regulaciones bancarias mexicanas que mencionaba anteriormente, nuestro grupo está tratando de identificar cuáles son las alternativas que estos carteles están utilizando por el hecho de que se ha vuelto más difícil para ellos ingresar en el sistema financiero mexicano. Creo que los oficiales de cumplimiento estadounidenses van a estar muy ocupados este año.

AT: ¿Qué clase de capacitación deberían recibir los profesionales de control legal para trabajar exitosamente con las instituciones financieras (IFs) o qué tipo de de capacitación deberían recibir las IFs para trabajar de manera efectiva con las autoridades de control legal?

DO: Yo mencioné anteriormente el Mercado Negro de Cambio de Pesos. Creo que sería bueno que los negocios tengan un conocimiento de qué es y cómo se lo implementa. Sea que usted se encuentre en el negocio de venta de computadoras, zapatos, ropa, o software, cualquier negocio podría ser objeto de un esquema del tipo del Mercado Negro de Cambio de Pesos. Creo que sería una ventaja para los oficiales de cumplimiento recibir capacitación sobre cómo los negocios tienden a estructuras estos fondos, qué clase de negocios generalmente participan, y cómo reportar adecuadamente a los clientes/negocios sospechosos y también cómo documentar mejor estas situaciones en los ROS. Cuanto mejor escriba el ROS el oficial de cumplimiento, más útil va a ser para el investigador.

AT: En sus 10 años en el área de control legal, ¿cuáles son algunas de las lecciones más importantes que aprendió?

DO: Una de las cosas más importantes que aprendí es "confiar en sus instintos". Si algo parece que no está bien y su instinto le dice que algo simplemente no encaja, lo más probable es que merezca que lo vuelva a revisar. Hay que confiar en esas evaluaciones iniciales, si ha estado en el negocio bastante tiempo, sea mi caso en el área de tráfico de drogas, o trabajando dentro de una institución financiera, hay que confiar en sus instintos y los de aquella gente que trabaja en las primeras líneas de su negocio.

Entrevista realizada por Karla Monterrosa-Yancey, CAMS, editora, ACAMS, editor@acams.org

Una guía para el control legal y las instituciones financieras:

El ALD y los desafíos de riesgo que enfrentan las instituciones financieras que emiten tarjetas prepagadas

Nota del editor: Éste es el primer artículo de una serie de dos.

Sea que sean utilizadas para ofrecer sustitutos costo-efectivos a los pagos tradicionales en papel, como los beneficios gubernamentales, descuentos y cuentas de ahorro flexibles, o para ofrecer un producto financiero a la comunidad que tiene poco acceso a los bancos o que no está bancarizada, la industria de las tarjetas prepagadas está creciendo rápidamente en los Estados Unidos y a nivel internacional. De acuerdo con una investigación encargada por MasterCard, Inc. y realizada por el Boston Consulting Group (BCG, por sus siglas en inglés), se espera que el valor total de la oportunidad de la tarjeta prepagada de esa marca en los EE.UU. supere los US$440.000 millones en 2017, casi el cuádruple de su valor estimado de US$120.200 millones en 2009. El estudio también muestra que el mercado de los EE.UU. continúa siendo el mayor segmento de tarjetas prepagadas de la marca en el mundo, con un 53 por ciento de participación en el mercado total. India, el Reino Unido, México, Italia, el Medio oriente y Brasil combinados, tendrán aproximadamente el 25 por ciento del mercado de tarjetas de marcas en 2017. Se espera que Brasil solamente se expanda de los US$1.700 millones en 2009 a más de US$17.000 en 2017.[1]

Si bien la mayoría puede estar familiarizada con los productos de tarjetas prepagadas que existen, incluidas las tarjetas de obsequio, de pago de sueldos y las recargables con fines generales, ¿tienen ustedes un buen conocimiento de qué controles ALD y de riesgo aplican las instituciones financieras antes de emitir o vender tarjetas prepagadas? La primera parte de esta serie de dos artículos estará dedicada a las consideraciones ALD y de riesgo específicamente de las instituciones financieras emisoras, seguida por la segunda parte, que se centrará en las consideraciones de aquellas empresas que desean comercializar y vender productos de tarjetas prepagadas. Un análisis de estas áreas le brinda a las autoridades de control legal un conocimiento de base par alas investigaciones presentas y futuras relacionadas con las tarjetas prepagadas.

En su mayoría, solo las instituciones financieras pueden ser miembros de las asociaciones de tarjetas, entendiéndose por ello que todas las tarjetas prepagadas son emitidas por una institución financiera. Si uno mira en el reverso de la tarjeta prepagada, verá la declaración del emisor. Hay dos caminos que las instituciones financieras pueden toma para emitir tarjetas prepagadas: (1) elaborar y emitir un programa de tarjeta prepagadas para comercializarla y venderla directamente a los consumidores mismos, o (2) asistir a terceros en la elaboración de programas de tarjetas prepagadas en donde la institución financiera sea el emisor pero el tercero sea el responsable de comercializarla y venderla a los consumidores. Esto es conocido típicamente como un modelo de auspicio y actualmente es el modelo preferido de la mayoría de las instituciones financieras. El tercero es conocido generalmente como el "gerente del programa" y la institución financiera es el "emisor".

Las instituciones financieras que tratan de participar en la industria del auspicio de prepagos, o que de hecho auspician a cualquier producto bancario incluidas tarjetas de crédito y otros productos de préstamo, deben poner un especial énfasis en la administración del riesgo de sus terceras contrapartes. En el pasado, las situaciones de "alquile un charter" fueron problemáticas para los reguladores y aún cuando la industria ha puesto en práctica importantes controles para evitar esta situación, los reguladores nuevamente están considerando severamente las prácticas de administración de riesgo de los terceros contraparte de las instituciones financieras. Además de las consideraciones contractuales, operativas y de riesgo financiero, el emisor debe considerar sus obligaciones de cumplimiento ALD. Al final del día, el emisor de la tarjeta prepagada es totalmente responsable del cumplimiento ALD de sus productos de la misma manera que con cualquier otro producto o servicio ofrecido bancario que se ofrezca. A continuación se indican algunas consideraciones específicas que las instituciones financieras deben tener presente para emitir tarjetas prepagadas.

Diligencia debida del gerente del programa

Si bien el emisor no está ofreciendo una tradicional cuenta corriente comercial al gerente del programa, está brindando acceso a los productos financieros. El emisor debería aplicar los mismos, sino mayores, programas de identificación del cliente (PIC) y estándares de diligencia debida reforzados (DDR) a los gerentes del programa que aplicaría a una cuenta comercial tradicional. Esto incluye tener la información completa sobre la compañía misma y sus dueños beneficiarios. También se recomienda tener los estados financieros, las políticas sobre seguridad de la información y recupero de desastres. Un buen programa de riesgo de terceros incluye un proceso de calificación del riesgo de los terceros, así también como los estándares de monitoreo basado en el riesgo y la revisión periódica de las relaciones con los terceros. Puede consultar los sitios web de las agencias regulatorias para obtener mayores guías sobre la administración del riesgo de los terceros.

Evaluaciones de riesgo ALD y OFAC

Las Evaluaciones ALD y de Riesgo OFAC amplias a nivel general de la empresa realizadas por el emisor deberían incluir la emisión de tarjetas prepagadas. La evaluación del riesgo no solo debería incluir la evaluación de los riesgos del producto, cliente y zona geográfica asociados con la nueva línea de negocios, también deberían incluir la evaluación del riesgo asociado con la oferta de productos a través de terceros. El Manual de Examen LSB/ALD del FFIEC de 2010 contiene un buen resumen de los factores de mitigación del riesgo que deberían considerarse.

Política ALD

Además de asegurarse que su Programa ALD a nivel general de la empresa incluya la emisión de prepagos, el emisor también debería tener obligaciones ALD documentadas que sus gerentes de programas deberían estar contractualmente obligados a cumplir. Estas obligaciones deberían incluir las expectativas que tiene el emisor sobre la política ALD del gerente del programa, los cuatro pilares y los requisitos específicos del PIC, el monitoreo de transacciones, el reporte y la OFAC. Dependiendo de las otras líneas de negocios del gerente del programa, el gerente de programa puede o no estar obligado a tener su propia política ALD para considerar las regulaciones ALD que le fueren aplicables. En esos casos, la venta de tarjetas prepagadas y las obligaciones del emisor deberían ser incorporadas a la política ALD existente del gerente del programa.

[1]Novedades de Pago (2010) Mastercad Publica Informe sobre Medición del Mercado de Prepagos, 12 de Julio de 2010 *(Payment News (2010), MasterCard Releases Prepaid Market Sizing Report, 12 July 2010)* www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html

Oficial ALD

Cada gerente de programa debería tener un oficial ALD designado. Dependiendo del tamaño de la compañía, el oficial puede tener varios cargos, incluido pero no limitado a los cargos legal, de fraude, riesgo, finanzas u operaciones. En todos los casos, el oficial ALD del gerente del programa debería tener los recursos necesarios para cumplir con sus responsabilidades; sin embargo, el oficial ALD puede tener una experiencia ALD limitada dependiendo de las demás líneas de negocios del gerente del programa. En esos casos, es beneficioso si el emisor puede brindar alguna capacitación adicional. También puede ser una ventaja para todos el ofrecerle al gerente del programa soluciones de capacitación, como las brindadas por la Asociación de Redes de Tarjetas Prepagadas de Marca (Network Branded Prepaid Card Association, o NBPCA, por sus siglas en inglés)[2] o ACAMS.

Capacitación ALD y agentes minoristas

Los gerentes de programa deberían estar obligados a asistir a capacitaciones iniciales y anuales sobre las obligaciones ALD del emisor. El gerente de programa debería estar obligados a brindar capacitación ALD al personal competente y a los agentes minoristas. Si el gerente del programa está utilizando agentes minoristas para vender o recargar las tarjetas prepagadas, es fundamental que el emisor se asegure que el agente minorista reciba capacitación ALD para la venta de sus productos. La manera de realizar esta capacitación debería ser una decisión basada en el riesgo; sin embargo, cuando sea posible, se recomienda que el emisor realice capacitación directa al agente minorista, en contraposición a la utilización del método de capacitación donde el gerente del programa de la capacitación. El emisor también debería tener un acuerdo contractual con cada agente minorista que vende sus tarjetas prepagadas.

Revisión independiente

El emisor debería asegurarse que su auditoria independiente anual incluya la revisión de sus programas y controles de las tarjetas prepagadas. El emisor también debería considerar la aplicación de obligaciones basadas en el riesgo para la revisión independiente de sus gerentes de programa. La revisión independiente es fundamental para que el emisor le muestre a su regulador que han realizado una supervisón adecuada del gerente del programa, y también puede ser utilizada para medir el desempeño para que el emisor evalúe el cumplimiento por parte del gerente del programa. En el caso de los gerentes de programa de mayor riesgo, el emisor puede obligar al gerente de programa a obtener una revisión independiente externa de su programa ALD y su cumplimiento de las obligaciones del emisor. En los casos de menor riesgo, el emisor puede optar por hacer su propia revisión del programa ALD del gerente del programa; sin embargo, idoneidad de esta revisión puede ser cuestionada por la participación del emisor en la fijación de los estándares. Una manera de resolver esto es que el emisor mantenga áreas o departamentos separados, uno para desarrollar y capacitar sobre los requisitos ALD y otro para realizar la revisión independiente para verificar el cumplimiento.

Programa de Identificación del Cliente

Una de las consideraciones ALD más importantes para el emisor es determinar cómo aplica mejor su Programa de Identificación de Clientes (PIC). Como institución financiera regulada, las obligaciones PIC del emisor respecto de las tarjetas prepagadas deberían ser similares a sus obligaciones PIC para los productos de depósitos tradicionales. En la mayoría de los casos, sin embargo, el PIC sobre los titulares de tarjetas prepagadas es realizado en un ámbito donde no hay contacto director personal con el cliente por la naturaleza en línea del producto o por restricciones a la seguridad de la información en el ámbito minorista. Dado que muchos gerentes de programas utilizarán métodos de verificación no documentales como las verificaciones en bases de datos públicas, el emisor debería considerar seleccionar y aprobar a algunos proveedores que cumplan con su criterio PIC y trabajar con esos proveedores para desarrollar un modelo de decisión PIC para que lo utilicen los gerentes de programas. Si el emisor no participara en la aprobación del método de verificación, será necesario incrementar la verificación de su PIC para asegurar que el gerente del programa cumpla con el mismo. El emisor también debería darle al gerente del programa sus requisitos para la verificación de la documentación, p.e. qué documentos son aceptables bajo su PIC. En el caso de los programas de pago de remuneraciones con tarjetas, el gerente del programa también puede solicitar aprobación para permitir que el empleador realice la verificación PIC. El emisor debe fijar y brindar estándares a ser aplicados también por el tercero. Sin embargo, si el emisor decide aplicar el PIC, es fundamental establecer un proceso de revisión para evaluar el cumplimiento por parte del gerente del programa con el PIC del emisor. Los emisores deberían considerar a las excepciones constantes y la omisión en el cumplimiento de las obligaciones PIC como una razón para rescindir el contrato.

> Cada gerente de programa debería tener un oficial ALD designado

Monitoreo y reporte de transacciones en efectivo

Los depósitos en efectivo, o "cargas de valor" son raramente aceptados por el emisor o el gerente del programa. Cuando las cargas de valor son aceptadas, generalmente es a través de una "red de carga" de un tercero, que tiene la correspondiente licencia para realizar transmisiones de dinero, así también como la responsabilidad para sumar y reportar las transacciones en efectivo. Además, por las características de las tarjetas prepagadas, no son transacciones sujetas a reporte, ya que las cargas y extracciones más elevadas están limitadas a US$2.500 por transacción. Sin embargo, los emisores deben tener en cuenta la capacidad para sumar las actividades en dinero en efectivo entre varios titulares de tarjetas. ¿Obtiene el emisor registros de las transacciones? Si es así, ¿cómo puede el emisor sumar las operaciones si un titular de tarjeta tiene una tarjeta con el gerente de programa A y otra tarjeta con el gerente de programa B? Estos temas de acumulación siguen siendo un reto para la industria de las tarjetas prepagadas.

[2]La NBPCA es una asociación sectorial abierta a todas las compañías que participan en la provisión de tarjetas prepagadas que incluyen un logotipo de red de marca y ofrece recursos educativos tanto a miembros como a no miembros. www.nbpca.org.

Necesidades de monitoreo de actividad sospechosa, reporte y control legal

El monitoreo de las actividades sospechosas puede ser realizado de una de dos maneras, dependiendo de la cantidad de información que reciba el emisor sobre sus titulares de tarjetas. Si el emisor recibe toda la información de los titulares de tarjetas incluida la información sobre las transacciones, conocida comúnmente como "archivos planos", puede monitorear la actividad dentro de su organización. El emisor puede utilizar una herramienta de fraude o ALD suministrada por una asociación de tarjetas, un sistema construido internamente y reglas basadas en el riesgo, o una solución externa de un proveedor. Sin embargo, actualmente existen pocas soluciones ofrecidas por vendedores para realizar el monitoreo ALD que consideren las características únicas de los programas de tarjetas prepagadas. También puede ser difícil justificar el costo de una solución ofrecida por un vendedor cuando el ingreso por tarjetas prepagadas puede ser mínimo por transacción.

Si el emisor no está recibiendo la información en archivos planos, o la información de las transacciones, debe hacerles cumplir a sus gerentes de programa obligaciones de monitoreo de actividades sospechosas. Los emisores deberían considerar el monitoreo para temas tales como las tarjetas múltiples, las cargas de valor en efectivo seguidas por extracciones en efectivo, créditos en comercios sin los correspondientes débitos, transferencias múltiples hacia y desde cuentas, depósitos realizados a nombre de personas distintas que el del titular de la tarjeta y cargas de valor por encima del promedio. El emisor también debería verificar periódicamente el cumplimiento por parte del gerente del programa con las obligaciones de monitoreo.

Como la institución financiera regulada, el emisor también tiene la responsabilidad de representar ROSs sobre las actividades sujetas a reporte. Las obligaciones ALD del emisor deberían suministrar a los gerentes de programas información como cuándo y cómo reportar actividades sospechosas al emisor. Los emisores deberían analizar el hacer que el gerente del programa reporte toda la actividad sospechosa, sin tener en cuenta los montos en dólares, o reportar las actividades sospechosas solo cuando se trate de operaciones sujetas a reporte en cuanto a su monto. Por ejemplo, si el gerente del programa solo está obligado a reportar actividades sospechosas que estén por encima del monto mínimo fijado, será poco probable que el emisor conozca a aquellos sospechosos que tengan varias tarjetas y que realicen actividades sospechosas que deberían ser reportadas una vez sumados los montos de todas las operaciones.

> El emisor debería completar el ROS con suficientes detalles para que las autoridades de control legal conozcan lo que ha sucedido

El emisor debería completar el ROS con suficientes detalles para que las autoridades de control legal conozcan lo que ha sucedido. Algunos funcionarios de control legal pueden tener escasa experiencia con las tarjetas prepagadas, por lo cual es importante utilizar terminología comprensible y explicar aquellos esquemas que son únicos de la industria. Por ejemplo, la industria de las tarjetas prepagadas utiliza el término "carga de valor", lo cual es, en efecto, un depósito. También es importante para las autoridades de control legal conocer la fuente de los fondos; si una tarjeta es cargada con dinero de la remuneración, el emisor debería informar el nombre del empleador. De la misma manera, si una tarjeta es cargada con dinero en efectivo, el emisor debería informar al comerciante que la carga, y la dirección, si la tuviere. El emisor también debería aplicar un proceso para responder a los pedidos de las autoridades de control legal, tanto a través de los de la sección 314(a), las órdenes judiciales y las Cartas de Seguridad Nacional. Muy poco se ha publicado sobre casos reales en los que hubiera actividad con tarjetas prepagadas; sin embargo, una buena fuente de información es el informe del GAFI publicado en octubre de 2010 titulado *Lavado de Dinero Utilizando Nuevos Métodos de Pago (Money Laundering Using New Payment Methods)*.

OFAC

Si bien están técnicamente separados de las regulaciones ALD, el emisor también debería asegurarse que sus gerentes de programa cumplan con las obligaciones OFAC. Se recomienda que los emisores realicen su propio monitoreo OFAC periódico para cumplir con sus obligaciones; sin embargo, tal vez no pueda realizar la verificación OFAC inicial antes de abrir la cuenta. En esos casos el emisor debe basarse en su gerente de programa para realizar la verificación inicial OFAC. El emisor debería informar al gerente de programa alas obligaciones en cuanto al plazo de la verificación, así también como las instrucciones sobre cómo descartar una falsa alarma y reportar cuando corresponda. El emisor debería incluir la verificación del proceso OFAC del gerente de programa como parte de su verificación PIC estándar. Finalmente, si bien las asociaciones de tarjetas requieren el bloqueo de ciertos países sancionados por la OFAC, también es una buena idea que el emisor entregue al gerente de programa su propia lista de países prohibidos.

Conclusión

Espero que este breve artículo les ofrezca información valiosa con relación al ALD y los desafíos de riesgo que enfrentan las instituciones financieras que emiten programas de tarjetas prepagadas. Si bien los retos pueden ser importantes, las tarjetas prepagadas siguen siendo una línea de productos viable para las instituciones financieras y un producto financiero necesario para un importante segmento de consumidores.

La segunda parte de este artículo estará dedicada a las consideraciones ALD y de riesgo para las empresas que venden y comercializan productos prepagados, incluidos algunos de los desafíos ALD presentados por el *Aviso de Regulación Propuesta sobre la Modificación a las Regulaciones de la Ley de Secreto Bancario* de FinCEN — *Definiciones y Otras Regulaciones Relacionadas con el Acceso Prepagado* (Notice of Proposed Rulemaking on *Amendment to the Bank Secrecy Act Regulations — Definitions and Other Regulations Relating to Prepaid Access*) publicado el 28 de junio de 2010.

Jani Gode, CAMS, consultor ALD senior, SightSpan, Inc. Mooresville, Carolina del Norte, EE.UU., jgode@sightspan.com

Riesgo cultivado en casa:
La creciente amenaza del fraude interno

Éstos son solo algunos casos sacados de recientes titulares de diarios. El desempleo, las deudas y la caída de la economía pueden influir para que los individuos cometan un delito. Una floreciente economía subterránea y esquemas altamente sofisticados están cambiando la cara del fraude interno.

Relaciones de la organización vs. relaciones individuales

Si bien la mayoría de las instituciones están concentradas en las amenazas externas, se han vuelto cada vez más vulnerables a quienes trabajan internamente *(insiders)* y son malintencionados: ex empleados o empleados actuales, contratistas, terceros en quienes se confiaba u otros socios comerciales que tienen acceso autorizado a la red, sistemas información u otros bienes de una institución. Celent, una firma de investigaciones y asesoramiento que presta servicios a la comunidad financiera, estima que aproximadamente el 60% de los casos de fraude bancario vinculados a una violación de la información o el robo de fondos son el trabajo de alguien que está dentro de la institución. Además del fraude, el sabotaje y el robo de propiedad intelectual también presentan serias amenazas internas.

Quienes cometen fraude interno han sido catalogados en algunos estudios por tener relaciones con la organización o relaciones individuales. Generalmente, aquellos que trabajan internamente y tienen relaciones con organizaciones tienen cargos que no son técnicos pero tienen acceso autorizado a los sistemas por sus puestos de trabajo. Están detrás de obtener ventajas financieras y generalmente cometerán el crimen mientras se encuentran en el lugar de trabajo.

Aquellos que trabajan internamente y tienen cargos técnicos o vinculados a ese aspecto, tienen relaciones individuales. Los consultores, contratistas y terceros en quienes se confía están incluidos en esta categoría porque puede utilizar sus conocimientos tecnológicos para producir un daño a la institución. Aquellos que trabajan adentro y tienen relaciones individuales generalmente cometen sabotaje o roban propiedad intelectual (bases de datos de client4es, códigos de propiedad de software, etc.). Los casos de sabotaje generalmente señalan ex empleados técnicamente eficientes que utilizan acceso no autorizado, remoto fuera del horario normal de trabajo mientras que el robo de propiedad intelectual general-

mente se comete durante el horario normal de trabajo por empleados actualmente en actividad y que tienen acceso autorizado. Las instituciones con programas de concientización más efectivos apoyan una visión más amplia del Conozca a Su Empleado (CSE). Estas instituciones tienen un mayor conocimiento de los delitos cometidos por aquellos que tienen relaciones con la organización en contraposición a los que tienen relaciones individuales.

Estadísticas alarmantes

En su *"Informe A Las Naciones Sobre el Fraude Y Abuso Ocupacional" de 2010 ("Report To The Nations On Occupational Fraud And Abuse"* la Asociación de Examinadores de Fraude Certificados *(Association of Certified Fraud Examiners*, o ACFE, por sus siglas en inglés) compiló información de aproximadamente 2.000 casos de fraude de todo el mundo que ocurrieron entre enero de 2008 y diciembre de 2009. El estudio reveló que los sectores que más comúnmente eran víctimas de esta situación eran los servicios bancarios/financieros, fabricación y administración gubernamental/pública. Según la información provista por los examinadores de fraude certificados que investigaron los casos, el informe presentó algunas estadísticas interesantes:

- Las organizaciones perdieron un estimado 5% de ingresos anuales por fraude. Cuando se aplica al Producto Bruto Mundial de 2009, esto se traduce en US$2,9 billones de posibles pérdidas por fraude.
- Casi un cuarto de esos fraude significó pérdidas de como mínimo US$1 millón.
- El plazo medio para la detección fue de 18 meses.
- El 90% de los casos analizados fueron esquemas con apropiación indebida de bienes.
- Más del 80% de los casos de fraude fueron cometidos por individuos que trabajaban en los sectores contable, de operaciones, ventas, gerenciamiento ejecutivo/superior, servicio al cliente o compras.

Reconociendo la creciente amenaza de fraude, el Pedido de Presupuesto para el 2010 incluyó un incremento de US$62,6 millones y 379 cargos adicionales para luchar más agresivamente contra el fraude hipotecario, el fraude corporativo y otros delitos económicos.

Análisis del riesgo del fraude interno

La globalización ha contribuido a la complejidad de las amenazas del análisis de las amenazas internas. Al evaluar el riesgo presentado por un empleado y un tercero, las instituciones deberían considerar los siguientes factores:

- Connivencia — los *insiders* pueden ser reclutados por o trabajar para gente externa como redes criminales u organizaciones y gobiernos extranjeros.
- Socios comerciales — el nivel de dificultad del monitoreo y control del acceso a la información y los sistemas se incrementa con los socios comerciales "de confianza".
- Fusiones y adquisiciones — existe un mayor riesgo cuando las organizaciones se fusionan con una organización adquirente.
- Diferencias culturales — es más difícil reconocer indicadores de conducta en un ámbito multicultural.
- Lealtades extranjeras — las organizaciones que operan fuera de su país de domicilio pueden tener empleados extranjeros que tengan otras lealtades.

Además, la cultura de la organización, las interacciones sutiles y las políticas y prácticas comerciales de la compañía deberían ser tenidas en cuenta en el análisis. Las instituciones que conocen el verdadero alcance y perfil del riesgo de fraude interno estarán mejor posiciones para proteger todos sus bienes.

Implementando una defensa agresiva

Si bien los expertos de la industria están de acuerdo en que la educación es la mejor defensa, la concientización a nivel general de la empresa es solo la mitad de la batalla. Se aconseja a las instituciones que un enfoque holístico es la una manera efectiva de detectar e impedir el fraude interno. Las recomendaciones para una estrategia holística contienen un enfoque de cuatro puntos fundamentales:

Organización — establecer una cultura proactiva y anti-fraude.

- Comenzar con el proceso de contratación; vigilancia y entrenamiento de los empleados nuevos
- Implementación de programas efectivos de concientización con reentrenamiento periódico de los empleados
- Monitoreo y respuesta ante las conductas sospechosas o negativas
- Anticipación y administración de los temas negativos de los lugares de trabajo

Políticas y Prácticas — documentar claramente y aplicar consistentemente las políticas y controles.

- Evaluar la amenaza de los *insiders*, los socios comerciales y los terceros de confianza en las evaluaciones de riesgo a nivel general de la empresa
- Elaborar un plan de respuesta ante incidentes de insiders que incluya un proceso confidencial y de "denunciante interno" seguro
- Intensificar las respuestas ante la presencia de actividades sospechosas
- Implementar claves estrictas y políticas de administración de cuentas sobre la base de lo que se necesite saber *(needs-to-know basis)*

Tecnología — crear rastreos y monitoreos unificados de ámbitos e información.

- Considerar las amenazas internas en el desarrollo del ciclo de vida del software
- Emplear tecnologías de autenticación e intrusión
- Ejercer un cuidado extra con los administradores y usuarios privilegiados
- Implementar controles estrictos para el intercambio de información

Clientes — aplicar educación constante sobre la prevención del fraude.

- Seminarios
- Políticas de privacidad
- Inclusión de declaraciones
- Placas con mensajes en el sitio web

La amenaza de la actividad criminal continúa aumentando con el aumento de esquemas de fraude más complejos. La División de Investigaciones Criminales del FBI informó al Comité Judicial del Senado de los EE.UU. que los casos nuevos de fraude corporativo aumentaron un 111% en 2010. El fraude interno sigue siendo uno de los puntos de mayor incremento, y, por lo tanto el área más grande de exposición para muchas instituciones. Definitivamente es el momento de tomar nota y repasar los planes y presupuestos del 2011 para lograr que la detección del fraude interno tenga la atención que merece.

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

Dentro de la mente criminal de cuello blanco

(Pronóstico predictivo o lectura de manos)

Al hacer mi investigación para este artículo, terminé yendo a una adivina. Quería ver qué tan bien podían predecir mi personalidad. Parecía que la precisión de las predicciones tenía una correlación inusual con la cantidad de dinero en efectivo que pagaba. Yo lo debía haber sabido, al hacer una lectura de cartas, él me siguió preguntando, ¿"saca una carta o se queda como está?" La síntesis por supuesto es que no existen métodos místicos o mágicos de pronósticos predictivos. Sin embargo, la historia es una gran maestra. El análisis de los criminales de cuello blanco reales puede brindar posibles señas, pistas e indicadores de eventos por ocurrir.

En la mayoría de las instituciones, monitoreamos la puerta de entrada y tenemos sospechas de los extraños (magnetómetro, rayos X, palpar el cuerpo) y monitoreamos la puerta de atrás previniendo incursiones (hackers, virus, phishers); sin embargo, los invitados, mejor conocidos como los empleados, raramente reciben una segunda mirada después de la fase inicial de contratación. Especialmente, cuanto más alto está una persona en la estructura, menor será el escrutinio que reciba. Esto puede contribuir a lo que a veces denominamos la desviación de la elite. Si bien la organización no convierte a la gente buena en mala, ellos pueden involuntariamente suscribir a la cultura que permite que los criminales de cuello blanco justifiquen en sus mentes la conducta desviada que cometen, y luego evaden tan hábilmente cualquier sentimiento de culpa por sus acciones.

La idea de tratar de entender la mente de un criminal de cuello blanco no se refiere a la habilidad de crear un listado modelo de señales de alerta de los hábitos personales de los empleados. El concepto es alentarle a usted a pensar acerca de las posibilidades de los tipos de riesgo asociados con cualquier elemento criminal dentro de su institución y sobre la oportunidad que pueda usted involuntariamente haber creado que permitió que esto ocurriera.

> ¿Cuál es la diferencia entre un crimen ocupacional y un crimen organizativo? Una definición reconocida comúnmente es que el crimen ocupacional es cometido en beneficio de un individuo y el crimen organizativo es aquél cometido en beneficio de una organización empleadora

Parte de lo que dificulta la elaboración de una evaluación del riesgo o pronóstico predictivo para los delitos de cuello blanco está enredado en el fundamento general de su existencia. Incluso la investigación del tema se vuelve confusa porque no hay ningún delito denominado "de cuello blanco". Por naturaleza, abarca muchas clases diferentes de delitos y varios tipos de autores. Probablemente estamos todos de acuerdo en que el tipo de Bernie Madoff ciertamente es el modelo. Pero ¿qué sucede con tipo de acá que da unos cheques sin fondos? ¿Sería calificado como un criminal de cuello blanco? ¿Qué pasaría en el caso del tipo que dirige un fraude de lotería desde su sótano?

Ayudaría tener alguna clase de definición de trabajo de qué se entiende por el término delito de cuello blanco (por lo menos para los objetivos de las instituciones financieras). Me gusta la siguiente definición dada por el Centro Nacional de Delitos de Cuello Blanco:

Actos Ilegales o poco éticos de engaño planeados por un individuo u organización, generalmente durante el curso de una actividad ocupacional legítima, por personas de status elevado o social respetable para beneficio personal o de una organización que violan la responsabilidad fiduciaria o la confianza pública.

A continuación de la definición anterior, y a los fines de este artículo, consideraremos a los delitos de cuello blanco como una clase de crimen ocupacional y/o de organización.

¿Cuál es la diferencia entre un crimen ocupacional y un crimen organizativo? Una definición reconocida comúnmente es que el crimen ocupacional es cometido en beneficio de un individuo y el crimen organizativo es aquél cometido en beneficio de una organización empleadora.

Para dificultar aún más la posibilidad de tener realmente un manejo cuantitativo de este tipo de compilación de datos, está el hecho de que muchas veces un delito de cuello blanco puede ser detectado y no reportado. Las instituciones pueden optar por no reportar un evento por la preocupación por su reputación y el daño que podría generarles. Nadie quiere ver el nombre de su institución en la tapa del The New York Times por indiscreciones embarazosas. Para agravar el asunto, un empleado que pudiera ser expuesto por la institución es liberado (sin intervención policial) solo para reaparecer en la institución de enfrente listo para reasumir la misma conducta delictiva.

Ahora que ya hemos establecido un marco semi-sólido sobre qué es un delito de cuello blanco, analicemos el concepto del pronóstico predictivo.

"Él está mintiendo cuando mira hacia abajo y hacia la izquierda" o "Le transpiraban las manos en una oficina donde hacía frío", o "Mírelo, está inquieto, debe estar nervioso porque es culpable". Estoy seguro de que todos han escuchado manifestaciones como esa, especialmente si ven algunos de esos ridículos programas de televisión sobre policías. Esos escenarios son todos bloques

individuales en donde se lee el lenguaje corporal y nadie y ni dos elementos son prueba de nada. Además, si está en el momento en que efectivamente está entrevistando a un sujeto y está tratando de leer su lenguaje corporal, entonces probablemente usted ya se dio cuenta y está meramente en un modo reactivo. El concepto aquí es tratar de reconocer a cierto perfil como una situación posiblemente problemática antes de tener que solucionar el problema.

La diligencia debida, especialmente al comienzo de cualquier relación de empleo, es esencial y puede ahorrarle a su compañía muchos problemas si usted tiene una estricta política de "conozca a su empleado". Habiendo dicho esto, desafortunadamente, puede no ayudar mucho en el área de los delitos de cuello blanco, ya que históricamente, aquellos que los cometen no tendrán antecedentes criminales. Esto podría deberse a varias razones como ser, que el sujeto nunca fue enjuiciado, el sujeto nunca fue atrapado o las instituciones anteriores no quisieron tener problemas. Elija una, pero al final lo que sucede es que, ahora el problema es suyo.

Analicemos el ámbito para que ocurra un delito de cuello blanco. Generalmente hay tres factores.

1. Un suministro generoso de inspirados y potenciales malhechores
2. Un objetivo que es un ámbito rico
3. La falta de sistemas y/o políticas de supervisión o control no efectivos

Centrándonos en la última categoría, que es lo único sobre lo cual usted tiene mucho control, podría ser el momento de realizar una revisión y análisis honesto de sus sistemas. En cuanto a lo que se refiere a la posibilidad de que un empleado se pase al lado oscuro, debería ser responsabilidad de la institución el conocer las situaciones e influencias externas que pudieran contribuir o empujar a un empleado en la dirección de cometer un delito. Me referiré a esto como "Continúe Conociendo a Su Empleado".

Ciertamente existen diferencias entre los perpetradores con bajo autocontrol que responden a un evento oportunista, gente que comete un delito para satisfacer a su propio ego, y aquellos que lo hacen dependiendo del estado de sus cosas personales. Ejemplos de influencias externas: cónyuge que es despedido del empleo, pago de la cuota del colegio de los hijos, apuestas en juegos de azar, temas de drogas y/o alcohol, divorcio y temas de salud.

Con la economía en mala situación y los 401K's convirtiéndose en 201K's, el no cobro de bonificaciones, reducciones en horas extras y en general con los pedidos a los empleados para que hagan más por menos, eso ciertamente podría contribuir a o disparar un evento inescrupuloso. Finalmente, la cultura corporativa juega un rol importante. Si la cadena de mando gerencial muestra una propensión a ser débil, perezosa o incluso a rayar en la falta de ética, entonces ciertamente la puerta se abre y seduce a algún empleado que podría estar contemplando cometer alguna actividad criminal.

En una cultura que es tan propensa a basarse en los resultados finales, es fácil pasar por alto el largo plazo. ¿Cómo hace la gerencia para observar cualquier potencial cambio en la personalidad o incluso conocer la situación personal de un empleado si existe una escasa comunicación entre ellos? No hay forma posible de tratar de pronosticar un evento de cuello blanco si no se tiene ninguna idea de quién es su empleado. Esto no significa que la gerencia deba invitar a todos a tomar una cerveza después de la oficina, pero debería hacer que la gerencia tome un rol más proactivo en el concepto dinámico del "conozca a su empleado". Muy pocos incidentes pueden arruinar la reputación de una institución financiera más rápido que el accionar de un mal empleado. El riesgo operativo lleva al riesgo reputacional.

Luego de analizar el ámbito, vayamos al meollo de esto y analicemos algunos de los factores de motivos e ideologías de una mente criminal de cuello blanco. Tengan presente que muchas de las cualidades siguientes están interrelacionadas y una persona puede exhibir varias y/o solo pocas o partes de todas ellas.

- *Codicia:* Esto es muy subjetivo. La codicia de una persona no es la misma que la de otra. ¿Realmente necesito cinco Ferraris? Sin embargo, el sujeto está motivado para obtener más y más objetos de su interés, sin tener en cuenta la necesidad o incluso el uso final del objeto. El deseo de tener riqueza es un apetito voraz.
- *Necesidad:* A diferencia de la codicia, un sujeto puede estar en un punto tan bajo que él ella siente que la única salida es robar. Apostar en juegos de azar, el alcohol o las drogas pueden ser las causas subyacentes; sin embargo, una vez que la puerta se abrió, empieza la cuesta abajo. Cuanto más tarde el sujeto en ser atrapado, más fácil será que continúe cometiendo delitos, aún mucho después de que el sujeto haya salido del pozo original. En otra variación de necesidad, el sujeto no puede admitir las equivocaciones en el lugar de trabajo y se vuelca al delito para ocultar esas deficiencias.
- *Imitación:* El sujeto se entera de que otras personas están cometiendo delitos, por lo que él/ella quiere demostrar que él/ella también puede hacerlo. La semiglorificación de los perpetradores por parte de varios medios de comunicación no ayuda en esto. La contratación de alguien que antes fue un delincuente para revisar sus sistemas puede tener algún mérito; sin embargo, puede tener un efecto de inspiración en el sujeto.
- *Resentimiento:* Un sujeto puede haber decidido que él/ella vale más que lo que cobra de salario, o siente que él/ella no ha sido tratado/a bien o que se le ha faltado el respeto de alguna manera o forma. Él/ella entonces siente que va a tomar lo que se merece.
- *Oportunismo:* A veces si las estrellas se alinean correctamente, la autodisciplina es baja y el oportunismo se revela, el sujeto asumirá el riesgo. Él/ella puede enamorarse de su particular estrategia financiera y volverse obsesivo/a con ella y decidido/a a probar que funciona. Cuando no es así, el oportunismo se convierte en necesidad.
- *Gratificación:* El dinero no es el factor motivante. El acto, en sí mismo, es lo que motiva al sujeto. El juego es lo más importante.
- *Validación:* El sujeto se perdona por sus propias acciones y cree que no ha hecho nada malo. Él/ella no se disculpan por sus acciones y cualquiera que haya salido perjudicado por sus acciones estaba equivocado por haberse cruzado en su camino. Él/ella siente poca o ninguna culpa. Él/ella puede deshumanizar cualquier hecho y creer que ninguna persona real fue perjudicada.
- *Superioridad:* Él/ella siente que él/ella es la persona más inteligente del lugar (y él/ella es muy inteligente) y él/ella tiene derecho a cualquier cosa que él/ella pueda obtener. El sujeto siente que él/ella está por encima de la ley, y ciertamente por encima de cualquier regla y regulación. Él/ella cree que él/ella tiene un propósito más elevado y no es necesario ser ético. Él/ella tiene el conocimiento de cómo funciona el sistema y puede actuar para no ser detectado.
- *Ego:* Una derivación de la superioridad, el sujeto busca una gratificación para su ego ganándoles a sus jefes, al sistema e incluso a las autoridades. Sin embargo, en el fondo de su ser existe un sentimiento de inferioridad que debe ser alimentado por los éxitos externos.
- *Dominio de Poder:* El sujeto ama el control y la admiración que conlleva. El sujeto se mueve en círculos de poder y se mezcla fácilmente con otros agentes de poder.
- *Adicción:* Al sujeto le gusta el riesgo y la adrenalina que va con él. Cada día que vence al sistema se necesitan conquistas nuevas crisis.
- Responsabilidad: Cuando las cosas van mal, no es culpa del sujeto. Puede culpar a los clientes por su ignorancia, o culpar a otros empleados, la organización o al gobierno por tener demasiadas o demasiado pocas regulaciones.
- Masa Crítica: El sujeto, cuando es confrontado y/o acorralado, tratará de redireccionar el tema fuera del tema real y dirigirlo a un tema diferente o incluso contra aquél que lo confronte. Esto le permite al sujeto mantener una perspectiva libre de culpa.

> Las instituciones deberían anticipar conceptos como la formación de equipos y el pensamiento crítico

En resumen, no existe un método de fuego seguro para determinar si una persona es o está por convertirse en un criminal de cuello blanco. Sin embargo, aquellos criminales que han sido capturados tienden a exhibir patrones de conducta similares. De la misma manera que con el uso de buenas técnicas de entrevista y de lectura del lenguaje corporal, no existe una única descripción de carácter que sea la panacea para el descubrimiento. Leer varias caracterizaciones de perfiles es simplemente crear bloques que cuando son agrupados crean nada más que posibles señales de advertencia.

La lección aquí es para la gerencia, la gerencia de nivel superior, la junta de directores, los dioses financieros o algún superhéroe que luche contra el crimen de cuello blanco, para que adopten un enfoque proactivo frente al delito de cuello alto. Las políticas y procedimientos escritos deberían ser preparados, desarrollados e implementados, y este riesgo debería ser administrado de la misma manera que lo haría con cualquier otra clase de riesgo. Las instituciones deberían anticipar conceptos como la formación de equipos y el pensamiento crítico. ¿Cómo se adapta al cambio? Observe sus propias conductas de confianza. Desarrolle estrategias para crear líderes y no simplemente gerentes. Cuanto más haga para conocer a su empleado, crear un aire de unidad, respeto mutuo y legalidad, entonces reducirá sus posibilidades de crear involuntariamente incidentes oportunistas.

Kevin Sullivan, CAMS, director de la Academia de Capacitación ALD, Ret. Inv. Policía del Estado de Nueva York, NY HIFCA El Dorado Task Force, Kevin@AMLtrainer.com

Association of Certified Anti-Money Laundering Specialists®

ACAMS®

7th Annual ACAMS

Anti-Money Laundering & Counter-Terrorism Financing Conference Europe

Mark Your Calendars

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

Register today for the most comprehensive training available featuring:

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

PLATINUM SPONSOR

DOWJONES

amleurope.org ▪ +1 305.373.0020 ▪ info@acams.org

Crimen organizado a la vuelta de la esquina

Lecciones aprendidas de enjuiciar a las bandas de fraude organizado

No importa la diferencia de su tamaño, ubicación geográfica, antecedentes o área de conocimiento, las organizaciones criminales que tienen como objetivo a las instituciones financieras se aprovechan de los vacíos en la capacitación de los empleados y la comunicación y las presiones que enfrentan los empleados de los bancos. A pesar de su usual falta de conocimiento sofisticado de la ley de Secreto Bancario (LSB) y el cuidado sobre los temas antilavado de dinero/Conozca a Su Cliente (ALD/CSC) que enfrentan las instituciones financieras, los criminales actúan en base a su conocimiento de la naturaleza humana y cómo explotarla mejor.

Hay cuatro áreas sobre las cuales las instituciones deberían ser especialmente precavidas: el proceso de aceptación de clientes, las respuestas a los reportes de las transacciones en las sucursales, las situaciones comprometidas de los empleados, y la interacción con el *call center*. Los patrones de hechos y las entrevistas de varias investigaciones y enjuiciamientos extensos de estos grupos ilustran los problemas y ofrecen soluciones para hacer que su institución sea un objetivo menos buscado.

Aceptación de clientes: mensajes confusos en la sucursal

El personal de la sucursal está bajo presión constante para abrir cuentas nuevas. Los empleados puede ser recompensados o penalizados, dependiendo de su éxito o fracaso en esta empresa. Mientras está bajo esta enorme presión, el personal de la sucursal también está obligado a asistir a capacita-

ciones sobre políticas y procedimientos ALD/CSC, incluidos aquellos relacionados con el proceso de aceptación o incorporación de clientes. La presión e incentive para abrir cuentas no siempre se lleva bien con las políticas y procedimientos ALD/CFT. Las bandas criminales dedicadas al fraude se aprovechan de este conflicto convenciendo a algunos empleados honestos — o ayudando a los deshonestos — para que abran cuentas para ellos violando la política del banco.

Entre los ejemplos de cómo los criminales abren cuentas fraudulentamente se incluyen:

1. Un banco donde los banqueros personales estaban autorizados a dejar la sucursal sin supervisión y se trasladaban a comunidades étnicas para firma la apertura de cuentas nuevas. Los banqueros eran responsables de analizar todos los documentos de identificación y de verificar la información.
2. Un gerente de sucursal que le permitió a un titular de cuenta en el banco traer los documentos de identidad de otras personas para abrirles las cuentas.
3. Cuentas personales y comerciales abiertas por la misma persona utilizando distintos nombres. Los titulares de las cuentas alegaron que eran conocidos por otros nombres en la comunidad internacional.
4. Cuentas abiertas a nombre de distintas personas no relacionadas, que no obstante compartían el mismo número telefónico, empleador o dirección.
5. Cuentas comerciales abiertas donde los domicilios de los negocios no existían o eran casillas de correo.

En cada ejemplo, se abrieron varias cuentas. Poco después de su apertura, las cuentas fueron utilizadas para cometer fraude con tarjetas de crédito, fraude con préstamos comerciales y personales y lavado de dinero. Dada la cantidad de cuentas abiertas, la banda criminal pudo movilizar menos dinero a través de cada cuenta y menos atención no deseada. Para el momento en que los sistemas ALD detectaron las cuentas y los bancos actuaron para cerrarlas, la banda defraudadora había robado varios millones de dólares en cargos impagos de tarjetas de crédito y préstamos de cada institución.

Muchos funcionarios de la industria han indicado que, como no hay riesgo de pérdida para el banco durante el proceso de incorporación del cliente, la transacción no es inherentemente riesgosa. Como se mencionó anteriormente, sin embargo, una vez que la organización criminal se ha infiltrado en la institución, su capacidad para cometer fraude es grande. Además, este fraude probablemente se extienda más allá del banco, donde la cuenta esté domiciliada, porque la siguiente institución descansará en el hecho de que el criminal tiene una cuenta en un banco al decidir si le permite abrir una cuenta u obtener un préstamo en su institución. El fracaso CSC de un banco puede, por ende, afectar adversamente a otros.

Brecha de comunicación: Departamentos ALD y la primera línea

Los cajeros de las sucursales y sus supervisores son los primeros en saber cuándo un titular de cuenta ha pedido algo inusual o ha dado una explicación que no tiene sentido. Ellos están familiarizados con las tendencias en su área e interactúan diariamente con potenciales criminales, titulares de cuenta honestos y viceversa. Una vez que consideran que algo no está bien, la sucursal genera un reporte de alerta. En la mayoría de los casos, sin embargo, ese reporte no es enviado a investigaciones sino al departamento ALD y/o de cumplimiento para decidir si hay que tomar alguna medida, incluida la presentación de un ROS. Los criminales se aprovechan de esto completando sus fraudes lo más rápido posible.

Por ejemplo, una banda dedicada al fraude especializada en obtener préstamos de Línea de Crédito de Vivienda (*Home Equity Line of Credit*, o HELOC, por sus siglas en inglés) de distintas instituciones sobre la misma propiedad residencial a través del uso de identificaciones fraudulentas y sin permiso del propietario. Cada préstamo fue aprobado por varios cientos de miles de dólares. Tan pronto como los préstamos se otorgaban, el objetivo comenzaba visitando a la sucursal local, casi todos los días, para cobrar cheques girados contra la cuenta HELOC. El monto de cada cheque era consistentemente menor a US$10.000. El personal de la sucursal encontró que esta conducta era inusual para el área y el tipo de cuenta. Presionaron al sujeto para obtener una explicación, y encontraron que había dado distintas y diversas respuestas. Los cajeros le informaron a su supervisor y enviaron un reporte de alerta referida a la actividad. Después de que el sujeto realizara numerosas visitas a la sucursal, el gerente conversó con él sobre el tamaño y la frecuencia de las extracciones. El sujeto respondió aumentando el monto de las extracciones de US$20.000 a US$30.000 por visita. Nuevamente, el personal de la sucursal siguió la política del banco y envió alertas sobre la conducta.

Para cuando alguien de investigaciones recibió el caso y conversó con el personal de la sucursal sobre sus alertas, las cuentas estaban totalmente vacías. Más aún, dado que el sujeto estaba utilizando documentos de identidad falsos, no había forma de identificarlo. Los funcionarios del banco dijeron que no habían respondido antes a los alertas porque el préstamo HELOC no era una transacción inherentemente riesgosa, ya que es el dinero del propio titular de la vivienda, garantizado por la propiedad. Se basaron en la evaluación del riesgo para excluir los alertas de los empleados. La banda dedicada al fraude robó más de US$1,4 millón.

Conozca a sus Empleados — Un asunto de confianza

Los postulantes a empleados son sometidos a investigación de varias maneras durante el proceso de selección. Una vez empleados, se utilizan métodos para monitorear la productividad y rastrear fondos apropiados indebidamente o cuando existen acusaciones de fraude. Pero existe una falta de revisión en tiempo real de los empleados nuevos o de los que ya lo eran para determinar si están participando en una conducta indebida antes de que la conducta se traduzca en una pérdida para el banco. Esto les da a las bandas criminales dedicadas al fraude la posibilidad de infiltrarse en la organización colocando un empleado nuevo de los suyos o comprometiendo a uno que ya era empleado.

Por ejemplo, una banda de fraude les paga a individuos jóvenes para que se postulen para cargos de cajeros a fin de robar información de los clientes. Después de una capacitación limitada, estos nuevos empleados a menudo tienen la posibilidad de acceder a casi todas las cuentas de todo el portafolio, incluidas las tarjetas de firma, sin restricciones numéricas, geográficas u otras restricciones. No se generan alertas aún cuando el empleado nuevo accede a cientos de cuentas sin hacer un seguimiento de las transacciones en ninguna de ellas. Estos nuevos empleados a menudo trabajarán solo unas pocas semanas y dejarán el empleo en el banco antes de que la banda criminal empiece a hacer extracciones no autorizadas desde las cuentas de los clientes a las que tiene acceso.

En el extremo opuesto del espectro se encuentran los empleados que llevan mucho tiempo trabajando en el lugar — a menudo

algunos han sido promovidos internamente. Están en puestos de confianza y las evaluaciones de sus desempeños tienden a destacar su productividad y no se concentran en si las cuentas que abrieron, o los préstamos que otorgaron, terminaron en fraude. La expectativa de que continúen produciendo, o alguna presión financiera externa, pueden hacer que sean susceptibles a los esfuerzos de las bandas criminales dedicadas al fraude y los comprometan.

Por ejemplo, un empleado que lleva mucho tiempo trabajando en la institución y que era gerente de una sucursal, desarrolló el hábito de la droga. Para tener dinero extra, comenzó a entrenar a un grupo de criminales sobre los procedimientos del banco con relación a los negocios de apertura de cuentas y obtención de préstamos. Asesoró a la banda dedicada al fraude respecto de los documentos que necesitaban e intercedió en su nombre ante el departamento de préstamos para asegurarse que los préstamos comerciales fueran otorgados, aún cuando sabía que no tenían ningún negocio legítimo. Por su tarea, recibía un porcentaje sobre cada préstamo que otorgaba. Como gerente de la sucursal, su nombre no aparecía en ningún documento de trabajo. Le dio la apertura de cuentas y el otorgamiento de préstamos a otro empleado de la sucursal. Ninguno de los préstamos, que totalizaron más de US$2 millones, fueron repagados jamás, y las cuentas fueron utilizadas para lavar dinero de la banda.

La revisión en tiempo real tanto de los empleados nuevos como de los antiguos habría ayudado al banco a identificar el fraude y a establecer quién era responsable. Una comparación de los registros de acceso del empleado y los cambios en la productividad de toda la sucursal, dentro de una zona geográfica limitada, o del portfolio, ayudaría a identificar cuando conducta anómala que pudiera resultar en una investigación posterior.

El call center — Ayuda a cualquier costo

Las bandas criminales necesitan que sus cuentas se mantengan abiertas a fin de lograr sus objetivos. Sin embargo, su conducta a menudo genera alertas ALD que congelan automática su actividad. Esto lleva al contacto entre los miembros de la organización criminal y el *call center*. Pero los empleados del *call center* no están entrenados en, ni son premiados por, identificar cualquier posible fraude. Incluso en los casos más extremos, donde quienes llaman no pueden responder correctamente a ninguna de las preguntas de seguridad, no hay ningún procedimiento para alertar a las áreas ALD, de cumplimiento o de investigaciones sobre las cuentas sospechosas.

Las bandas criminales dedicadas al fraude se aprovechan de la naturaleza human y el deseo del empleado del call-center de ayudarles a fin de continuar con su fraude.

> Las bandas criminales necesitan que sus cuentas se mantengan abiertas a fin de lograr sus objetivos

Algunos ejemplos incluyen:

1. Una persona que llama y que indica que no tenía su número de cuenta o la fecha de nacimiento con ella, sin embargo logró que se eliminara la suspensión de su tarjeta de crédito;
2. Los miembros de la banda dedicada al fraude que se avisaron entre sí para estar en línea con el *call center* y seguir disculpándose "hasta que te atiende una señora amable que se lamenta por ti";
3. Una persona que llama y que no puede indicar su dirección o número telefónico, incluso después de que el empleado del *call center* le diera algunas pistas, aún así, sus tarjetas de crédito no estaban congeladas;
4. Las personas que llamaron y que estuvieron en el teléfono durante más de una hora y fueron transferidas a distintos representantes antes de que se les reactivaran sus tarjetas sin haber respondido correctamente a ninguna pregunta;
5. Una persona que llamó y se negó a que el representante del *call center* le enviara a alguien a su negocio para verificar su máquina comercial pero aún así logró que su cuenta fuera reabierta;
6. Una persona que cobró casi US$20.000 en anticipos en efectivo sobre una tarjeta de crédito nueva sin ninguna explicación pero sobre quien se eliminó el alerta de fraude simplemente llamando al *call center*.

Por supuesto, una vez restablecidas, todas estas cuentas fueron utilizadas para cometer fraude con tarjetas de crédito y lavado de dinero. Ninguno de los *call centers* parecía saber qué hacer con una persona que llama y que no pudo responder a ninguna pregunta, una cuya identidad fue cuestionable, o que actuó irracionalmente. Al final de las llamadas, el representante simplemente restableció o reactivó las cuentas. Así, los sistemas ALD basados en el riesgo fueron neutralizados efectivamente por los *call centers* de atención al cliente. Si hubiere un mejor entrenamiento para identificar y dirigir a estos posibles defraudadores que llaman allí, y se aplicara un sistema basado en premios para los empleados de los call-centers, estas instituciones habrían sido mucho más exitosas en la prevención del fraude.

¿Qué puede hacer para proteger mejor a su institución?

Preste atención al proceso de incorporación del cliente. Si las bandas criminales dedicadas al fraude no pueden poner un pie en su institución, no pueden defraudarlo tan fácilmente y se irán a otro lado. Las revisiones en tiempo real de los empleados también pueden reducir la posibilidad de sus empleados de ayudar a la banda fraudulenta. Si los empleados nuevos pueden ser detectados — por acceder a demasiadas cuentas con relación a sus compañeros de trabajo, sus ubicaciones geográficas o sus puestos — y los empleados más antiguos pueden ser detectados — por un súbito cambio en la productividad — las bandas fraudulentas pueden ser detenidas más rápido. Una revisión del incumplimiento de un préstamo y de una tarjeta de crédito también puede brindarle a la institución información sobre un posible empleado comprometido.

Finalmente, el desarrollo de una línea de emergencia y un sistema de recompensas en donde el personal de la sucursal y del *call center* pueda rápida y fácilmente alertar sobre investigaciones acerca de algo que está fuera de su normal experiencia con el cliente y sobre un posible fraude, le daría a la institución un método que no solo pueda detener un fraude en curso, sino que posiblemente pueda identificar al defraudador para llevarlo ante las autoridades de control legal.

Meryl Lutsky, directora, Unidad de Lavado de Dinero, Oficina del Fiscal General del Estado de Nueva York, Nueva York, Nueva York, EE.UU. meryl.lutsky@ag.ny.gov

Tráfico de personas: El dilema del ALD

Un tema sorpresivo hizo su aparición en la conferencia anual de ACAMS en Las Vegas en Septiembre. Y el rumor es que el mismo tema fue muy destacado en la conferencia de ABA en Washington, DC en Octubre. El tráfico de personas, un tema raramente mencionado en los círculos antilavado de dinero, se ha convertido en un tema "candente" de sumo interés. El tráfico de personas es probablemente el delito subyacente más subrepticio en surgir desde el comienzo de la obligación de presentación del reporte de operación sospechosa (ROS) con miles de millones de dólares generados anualmente en sus diversas formas. Con esa clase de crecimiento, cualquier nivel de apoyo que los profesionales antilavado de dinero (ALD) puedan brindarles a las autoridades de control legal para identificar el lavado de dinero resultante del tráfico de personas es invalorable.

"Después del tráfico de drogas, el tráfico de personas está vinculado con el tráfico ilegal de armas como la segunda industria delictiva más grande del mundo, y está en rápido crecimiento".[1] Aunque el tráfico de personas se extiende en los continentes, la definición de los indicadores de las señales de alerta financieras del tráfico de personas es un reto extremo porque presenta diversas formas.

Para elaborar los indicadores del tráfico de personas, debe definirse la actividad ilegal misma. Primero y antes que nada, el tráfico de persona no es lo mismo que el contrabando de personas. Aquellos que son contrabandeados consienten su situación de una u otra forma, mientras que el tráfico implica el uso de la fuerza/coerción contra la víctima. El tráfico no necesariamente implica el movimiento físico de la víctima, mientras que en el contrabando se produce el movimiento transnacional o internacional.

El "Protocolo para Prevenir, Suprimir y Castigar el Tráfico de Personas, especialmente de Mujeres y Niños" es un protocolo de la Convención contra el Crimen Organizado Transnacional, uno de los dos "protocolos de Palermo" adoptados por las Naciones Unidas en Palermo, Italia, en 2000. Firmado por 116 países, el Protocolo sobre el Tráfico entró en vigencia en diciembre de 2003[2].

De acuerdo con el protocolo sobre Tráfico, el tráfico de personas es definido como:

"(a)… el reclutamiento, transporte, transferencia, ocultamiento o recepción de personas, por medio de la amenaza o el uso de la fuerza u otras formas de coerción, de secuestro, de fraude, de engaño, del abuso de poder o de una posición de vulnerabilidad o de la entrega o recepción de pagos o beneficios para lograr el consentimiento de una persona por parte de una persona que tenga el control sobre otra persona, con el objeto de cometer la explotación de ella. La explotación incluirá, como mínimo, la explotación de la prostitución de otros u otras formas de explotación sexual, trabajo o servicios forzados, esclavitud o prácticas similares a la esclavitud, servidumbre o extracción de órganos;

(b) El consentimiento de una víctima de tráfico de personas de la explotación buscada indicada en el subpárrafo (a) de este artículo será irrelevante cuando se haya utilizado cualquiera de los medios indicados en el subpárrafo (a);

(c) El reclutamiento, transporte, transferencia, ocultamiento o recepción de un niño con el objeto de explotarlos será considerado "tráfico de personas" aún si esto no implica a ninguno de los medios indicados en el subpárrafo (a) de este artículo;

(d) "Niño" significa cualquier persona menor de dieciocho años de edad".[3]

La Ley de Protección de las Víctimas del Tráfico y Violencia de 2000 (TVPA, por sus siglas en inglés) define al tráfico de personas dividiendo a la actividad ilegal en dos subgrupos: tráfico severo de personas y tráfico sexual.

"(1) El término "formas severas de tráfico de personas" significa

(A) Tráfico sexual en el cual un acto sexual comercial es inducido por la fuerza, el fraude o la coerción, o en el cual la persona inducida a realizar tal acto no tiene 18 años de edad; o (B) el reclutamiento, ocultamiento, transporte, provisión u obtención de una persona para que realice trabajos o servicios, a través del uso de la fuerza, fraude o coerción con el objeto de someterla a servidumbre involuntaria, trabajos de peón, esclavitud por deuda, o esclavitud.

(2)…El término "tráfico sexual" significa el reclutamiento, ocultamiento, transporte, provisión u obtención de una persona con el propósito de un acto sexual comercial".[4]

De las definiciones indicadas, solo un menor de 18 puede ser víctima de un "tráfico severo" cuando sea traficado con el propósito de sexo comercial bajo la TVPA, mientras que el protocolo sobre Tráfico no hace esa distinción. Si bien el protocolo sobre Tráfico prohíbe explícitamente el comercio de órganos humanos cuando el donante es coaccionado y por ello considera a esto tráfico humano, la TVPA no considera al tráfico de órganos humanos como tráfico de personas. Otra anomalía es que las adopciones ilegales no son consideradas, por cualquiera de las definiciones, como tráfico de personas a menos que la adopción ilegal llegue a ser servidumbre involuntaria (p.e., esclavitud) porque carece del uso de la fuerza, el fraude o la coerción para obligar a prestar servicios al niño adoptado ilegalmente.

Aunque la definición exacta del tráfico de personas puede no ser consistente en todos los actos, las definiciones sí están de acuerdo en muchas de las actividades subyacentes incluidas en el tráfico de personas. El secuestro es tráfico de personas. La prostitución forzada es tráfico de personas. El trabajo forzado/la servidumbre es tráfico de personas.

Las investigaciones sacaron a la luz sorprendentes y, honestamente, perturbadoras imágenes del tráfico de personas sin importar qué definición se utilice. Además de los

[1]http://www.acf.hhs.gov/trafficking/campaign_kits/tool_kit_law/law_enforcement.ppt#287,3,Human Trafficking: What Is It?
[2]http://www.state.gov/documents/organization/142979.pdf
[3]http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_%20traff_eng.pdf
[4]http://www.state.gov/documents/organization/10492.pdf

métodos atroces con los cuales se realiza el tráfico, los distintos métodos utilizados para controlar a las víctimas son igualmente inquietantes incluyen:

- *Físico:* palizas, quemaduras, violaciones y privación de alimentos
- *Emocional:* aislamiento, abuso psicológico, dependencia de drogas y amenazas contra miembros de la familia en los países de origen
- *Financiero:* servidumbre por deuda y amenaza de deportación.[5]

Habiendo identificado a los delitos subyacentes del tráfico de personas, uno podría pensar que la identificación de los indicadores de las señales de alerta de la actividades deberían ser bastante simples. No es tan así.

Las características de las posibles víctimas han sido identificadas y han sido ampliamente publicadas en sitios de Internet dedicados a combatir el tráfico de personas. Una lista de indicadores de señales de alerta sobre las víctimas puede consultarse en el sitio http://nhtrc.polarisproject.org/call-the-hotline/identifying-human-trafficking-.html#who. No es de sorprender que la investigación no pudiera encontrar una lista publicada de indicadores de transacciones asociados con el tráfico de personas que pudiera ser volcada en un indicador de actividad sospechosa (IAS) para la detección automática de tal actividad. Lo que la investigación sí respaldó es la afirmación de que los funcionarios locales de control legal, no los investigadores ALD, son los más proclives a descubrir el tráfico de personas.[6] Entonces, ¿qué se conoce sobre el tráfico de personas que pueda ayudar en la definición de las transacciones financieras que pudieran acompañar a esa actividad?

- El tráfico de personas ha sido identificado en las siguientes industrias: trabajadoras domésticas (niñeras, mucamas), paisajismo, salones de manicuras, restaurantes, limpieza industrial, construcción, hospitalidad, ventas de revistas y flores, agricultura, fábricas (confección de ropa, etc.).[7]
- Las víctimas no reciben un pago por sus servicios o reciben remuneraciones sensiblemente menores por sus servicios.
- Los traficantes de personas muy a menudo están asociados con otros delitos (p.e., prostitución, pornografía, abuso doméstico, lesiones y negocios ilegales).
- Las víctimas pueden no ser "compradas" pero pueden ser raptadas o vendidas por los progenitores u otra parte responsable (p.e., proxeneta).
- Las víctimas pueden estar trabajando para pagar deudas que datan de generaciones anteriores.
- El año pasado, el mundo importó y exportó miles de millones de dólares en productos manchados por el trabajo forzado en la fabricación y obtención de materias primas, según la Organización Internacional del Trabajo (OIT). El trabajo forzado también es común en las industrias del algodón, chocolate, acero, caucho, estaño, tungsteno, caña de azúcar y mariscos.

Los últimos tres elementos indicados hacen que el lema "siga el dinero" en los casos de tráfico de personas sea extremadamente difícil. Las víctimas secuestradas son la fuente de los futuros fondos ilícitos, si llegan a ser integrados en el sistema bancario a través de depósitos bancarios regulares de negocios con manejo intensivo de dinero en efectivo, pueden no llegar a ser rastreados nunca al delito original de tráfico.

Las víctimas que trabajan para pagar deudas que datan de generaciones anteriores, si trabajan en un negocio legítimo, teñirían de ilegalidad cualquier ganancia producida por el negocio. Similar al último punto, la identificación de las víctimas traficadas que están siendo utilizadas para generar materias primas o productos finales de compañías legítimas es una propuesta de enormes proporciones para cualquier programa ALD. En todos los aspectos, los fondos que se mueven a través de la cuenta bancaria de una compañía legítima aparecerían sin manchas, intachables. El negocio funciona como cualquier otro negocio.

Un indicador, sobre el cual un Investigador ALD de un banco puede no tener una línea clara a la vista, sería si los impuestos por salarios y/o los salarios no coinciden con los gastos que se espera tenga una empresa con una actividad similar. Sin embargo, en una época en donde las compañías tienen operaciones bancarias con múltiples instituciones financieras y donde las corporaciones multinacionales tienen mega-subsidiarias, la determinación de los salarios adecuados y/o de los impuestos sobre las remuneraciones para una compañías con una producción determinada puede no ser, y probablemente no sea, factible.

[5]http://www.fbi.gov/news/stories/2006/june/humantrafficking_061206
[6]http://www.acf.hhs.gov/trafficking/campaign_kits/tool_kit_law/law_enforcement.ppt#272,19,Identifying Crime of Human Trafficking
[7]http://nhtrc.polarisproject.org/call-the-hotline/identifying-human-trafficking-.html#who

Otra señal de alerta de que algo no está bien es cuando varios empleados indican el mismo domicilio comercial como su dirección particular. Esto puede ser un indicador de que los empleados no tienen una residencia documentada. Para las instituciones financieras, el campo visual de que los domicilios residenciales de los empleados de los clientes no es necesariamente transparente e incluso sería más obstaculizados para llegar a las víctimas del tráfico de personas ya que las pistas documentales que llevan a las víctimas, como los cheques y los cheques de pago de remuneraciones, son evitados para asegurarse que esa actividad no sea detectada. Generalmente, los traficantes no crearán cuentas a nombre de las víctimas; por lo tanto, los pasos del programa de identificación del cliente (PIC) y otras validaciones para la apertura de cuentas que de otra manera pudieran colaborar en la identificación de una tendencia negativa, como la información de una dirección comercial, no son aplicables.

De hecho, el Informe de Tipologías del Grupo de Trabajo sobre Lavado de Dinero & Financiamiento del Terrorismo del GAFI de 2004 – 2005 confirma "No se ha identificado ninguna técnica nueva de lavado de dinero que pueda ser asociada únicamente con estos delitos. Aunque el sistema de reporte de ROS general algunas investigaciones, el tráfico de seres humanos y de inmigrantes ilegales sigue siendo fundamentalmente un tema de control legal".[8]

Aunque no existen señales de alerta comunes para todos los casos de tráfico de personas, un caso reciente de control legal en los Estados Unidos ha identificado el uso de "cuentas conducto"[9] (cuentas conducto) para perpetuar el flujo de dinero en una importante operación de tráfico (ver cuadro sobre información de cuentas conducto).

Los traficantes de personas recientemente han comenzado ha recibir una prensa negativa ampliamente difundida que los jefes del tráfico de drogas, los defraudadores con esquemas Ponzi y los evasores fiscales han cosechado en los círculos antilavado de dinero. Algunos resonantes arrestos muy recientes aumentan el disgusto del público estadounidenses y requieren medidas al especto. La pregunta sigue vigente, ¿los profesionales antilavado de dinero son los "primeros en responder" adecuados ante esta tormenta de fuego? La respuesta: probablemente no.

John Byrne, vicepresidente ejecutivo de ACAMS expresa que "el tráfico de personas es un delito que resuena en todos lados. El tráfico ocurre en todos lados alrededor nuestro y pide una respuesta". Byrne también manifestó que ACAMS es el foro perfecto para llevar a cabo discusiones abiertas con las autoridades de control leal sobre cómo los profesionales antilavado de dinero pueden colaborar en la detección de un delito que no necesariamente esté basado en el dinero. Con más de 10.000 miembros, ACAMS continuará brindando guías útiles y respuestas serias a las autoridades de control legal, ya que ellas dirigen el esfuerzo para erradicar este horrible delito. Además, ACAMS creó un sitio web dedicado a luchar contra el Tráfico de Personas y el Contrabando de Personas en Noviembre de 2010.[10]

Además de la dificultad en descubrir y enjuiciar exitosamente los casos de tráfico de personas, también se da que muchas víctimas dudan en denunciar la situación

Además de la dificultad en descubrir y enjuiciar exitosamente los casos de tráfico de personas, también se da que muchas víctimas dudan en denunciar la situación. Con el paso del tiempo, la víctima puede efectivamente percibir a sus traficantes o nuevo "dueño" como su salvador, alguien en quien confiar y de quien depender. El traficante o dueño atiende las necesidades básicas de la víctima (alimentos, alojamiento, ropa). Cuando la víctima es un niño, emociones conflictivas como la relación con el traficante, el temor al castigo y un deseo inherente de confiar en los adultos puede impedir el reporte, incluso en aquellos pocos casos en los que el reporte es factible. En algunos casos, el tráfico es aceptado y alentado ampliamente (piense en los matrimonios forzados), lo cual esencialmente extingue cualquier esperanza de rescate por parte de la víctima.

La educación y el soporte son los roles definitivos que los oficiales antilavado de dinero deberían asumir a medida que el drama del tráfico de personas sigue extendiéndose. Como con cualquier tema candente, los profesionales ALD deberían tomar esta oportunidad para validar sus procesos de detección y programas de capacitación apara asegurarse que la información relacionada con las tipologías del tráfico de personas sea considerada para su integración correcta en los programas ALD. Debido a que es poco probable que se desarrolle un escenario automático de detección específica para descubrir indicadores de actividades de tráfico de personas, la integración puede consistir solamente en la educación del personal sobre las actividades subyacentes del tráfico para fomentar un conocimiento general. La capacitación efectivo que incorpora la información sobre las señales de alerta como las listas de remuneraciones al personal o los impuestos que no se condicen con los niveles de personal y las características de las cuentas conducto adquieren una importancia adicional para los investigadores.

Mientras que el tráfico de personas sigue siendo un tema de derechos humanos, los profesionales ALD pueden ciertamente dar apoyo moral a la causa incrementando la concientización y el conocimiento de que el tráfico es el delito subyacente de algunas actividades sujetas a reporte de ROS consideradas a diario. Los investigadores de las instituciones financieras deben continuar reportando operaciones o actividades sospechosas o inusuales para brindar las pistas necesarias que las autoridades de control legal utilizarán para encontrar a los traficantes de personas.

Jean-Ann Murphy, CAMS, EE.UU., envíe sus comentarios a editor@acams.org

[8]http://www.acams.org/ACAMS/ACAMS/UploadedImages/pdf%20downloads/HT/FATF-GAFI_Document.pdf
[9]Información entregada por una importante institución financiera
[10]http://www.acams.org/ACAMS/ACAMS/topics/humantrafficking/Default.aspx

Secretos Oscuros del Tráfico de Personas:

- Las familias a veces calculan cuánta deuda pueden asumir basándose en sus miembros integrantes *vendibles*.[11]
- *Millones* de víctimas del tráfico están trabajando para pagar las *deudas de sus ancestros*.[12]
- *100.000 niños estadounidenses* son obligados a ejercer la prostitución cada año *en los EE.UU.*[13]
- Todos los días productos como teléfonos celulares, anillos de bodas, computadoras laptop y baterías son fabricadas con minerales obtenidos con el trabajo de personas sometidas a esclavitud en el Congo del Este, donde existe el trabajo forzado, la servidumbre por deudas, niños trabajando en condiciones peligrosas, casamientos forzados y abuso sexual infantil.[14]
- El ciudadano promedio probablemente ha ayudado inadvertidamente a los traficantes de personas. Todos los días cientos de productos son fabricados con trabajo forzado y/o trabajo infantil. Ver la lista de 122 productos en: http://www.dol.gov/ilab/programs/ocft/PDF/2009TVPRA.pdf

CUENTAS CONDUCTO[15]

Las cuentas conducto es un término relativamente nuevo en los círculos antilavado de dinero. Aunque el uso de las cuentas conducto se descubrió en un importante caso de tráfico de personas, los investigadores y los profesionales antilavado de dinero no pueden perder de vista que el tráfico de personas existe en tantas formas que los hechos identificados en un caso no deberían ser interpretados como que todos los casos de tráfico usarían el mismo tipo de vehículo financiero. Además, cuando se identifica la actividad de la cuenta conducto, los investigadores no pueden asumir que se ha descubierto una situación de tráfico de personas. Si bien muchos de los factores indicados a continuación considerados individualmente pueden representar una actividad inusual/inesperada, cuando son considerados en combinación, la posibilidad de que la actividad identificada represente alguna forma actividad ilegal, y por ende de actividad que deba reportarse, se incrementa significativamente.

- Las cuentas conducto no solo son indicadores de tráfico (p.e., también son utilizadas en casos de contrabando)
- Las cuentas son abiertas como cuentas personales o comerciales; las cuentas podrías ser cuentas de ahorro o corrientes
- Las cuentas son abiertas con menos de US$500, y a los pocos días se realizan depósitos de grandes sumas de dinero en efectivo
- Los depósitos consisten casi exclusivamente de depósitos de dinero en efectivo de grandes sumas de dinero de cifras redondas (p.e., US$1800, US$2000) realizados en otros estados excepto Arizona
- Los depósitos son realizados en lugares distintos de los cajeros de la sucursal (lugares lejanos, cajeros automáticos) por parte de depositantes no identificados
- En los casos en donde los depositantes fueron identificados, los depositantes generalmente no eran clientes del banco, y a menudo se utilizando direcciones mexicanas
- Los depósitos no tienen relación con el empleo indicado — los cuales a menudo son "niñera" "paisajista" o "desconocido"
- La actividad se realiza fuera del estado donde se abrió la cuenta
- En los estados donde se hicieron los depósitos no se realiza/espera otra actividad normal
- No hay actividad periódica rutinaria en la cuenta — como el depósito del cheque del pago de salarios, alquiler, pagos de facturas de servicios o extracciones periódicas de dinero en efectivo
- Todas las extracciones se realizan en distintas sucursales en Arizona o inmediatamente al sur de Arizona en las ciudades fronterizas mexicanas, a menudo a través de varias extracciones de grandes sumas de dinero de cajeros automáticos, extracciones de efectivo en cajeros o cheques de banco
- Las cuentas generalmente son abiertas durante menos de un año o dejan de tener movimiento y casi no tienen saldo

[11]http://www.state.gov/documents/organization/142979.pdf
[12]http://www.state.gov/documents/organization/142979.pdf
[13]http://humantrafficking.change.org/blog/view/urgent_need_to_support_critical_services_for_americas_sex_trafficked_children
[14]http://humantrafficking.change.org/blog/view/sec_asks_america_whats_your_solution_for_conflict_minerals
[15]Representantes del Departamento de Seguridad Interior y la Oficina Federal de Investigaciones solicitaron que la siguiente información sobre las cuentas conducto fuera incluida en el artículo sobre Tráfico de Personas

La tarjeta prepagada — Crecimiento en su uso y riesgo

En los últimos años, los productos de tarjetas prepagadas han emergidos en el centro del sistema financiero de los EE.UU. a un ritmo cada vez mayor. FinCEN estima que hay más de 2,5 millones de tarjetas prepagadas nuevas emitidas cada año, y se estima que existe una red de 7,5 millones de tarjetas en uso de empresas como Visa o MasterCard.[1] Las tarjetas prepagadas han experimentado una tasa de crecimiento del 35% desde 2004, de los US$64.000 millones en cargas anuales a más de US$178.000 millones, según la información brindada por MSN Money Tool.[2] La seguridad y conveniencia de los productos prepagadas parece haber sido aceptada y adoptada por muchos consumidores.

La popularidad de las tarjetas prepagadas ha sido generada por varios factores que están principalmente vinculados con los esfuerzos para ofrecer productos financieros costo-efectivos a individuos que, o no operan con ningún banco, o pueden acceder a pocos productos bancarios. Además, las tarjetas prepagadas son utilizadas por los empleadores, los gobiernos federal, estatal y local como método de pago — las tarjetas pueden ser recargadas fácilmente con distintos montos para adaptarse a una variedad de necesidades de pago. El acceso y la conveniencia de las tarjetas prepagadas han hecho que se tenga acceso a las ventajas de operar con bancos posiblemente para casi todos, y la ampliación de las oportunidades bancarias financieras.

Desafortunadamente las tarjetas prepagadas no son inmunes a los riesgos – muchos de los mismos factores que hacen que el acceso y uso prepagado sea tan atractivo para los consumidores también hacen que sea vulnerable ante las actividades ilícitas.

[1]Departamento del Tesoro de los EE.UU. (2010). Modificación de la ley de secreto bancario (31 CFR Parte 103). Washington, DC: Obtenido de http://www <http://www/>. fincen.gov/statutes_regs/frn/pdf/Prepaid%20Access%20NPRM.pdf <http://fincen.gov/statutes_regs/frn/pdf/Prepaid%20Access%20NPRM.pdf>

[2] BusinessWeek. Lo esencial de las tarjetas de obsequio prepagadas: herramienta terrorista. Obtenida de http://moneycentral.msn.com/content/Banking/P137668.asp?Printer

Los riesgos y vulnerabilidades de las instituciones financieras pueden estar vinculados principalmente con el anonimato propio y con la relativa facilidad para acceder a fondos y realizar operaciones con una tarjeta prepagadas. Esta combinación de factores de riesgo crea la posibilidad de un volumen importante de dinero trasladándose a través de múltiples productos — todo con "dueños" o "beneficiarios" desconocidos. Además, el anonimato de las tarjetas prepagadas ofrece una ventaja a los individuos con intenciones dudosas, ya que pueden realizar transacciones con importantes sumas de dinero y a la vez tener la posibilidad de evitar algunas de las obligaciones de reporte de dinero en efectivo, compras con dinero en efectivo y de conservación de registros a las cuales una cuenta no prepagada podría estar sujeta.

Los ejemplos de estos reportes incluyen el Reporte de Operación en Efectivo, la Compra o Venta de Instrumentos Monetarios, el Reporte de Transporte Internacional de Dinero en Efectivo o de Instrumentos Monetarios y otros reportes establecidos por FinCEN – cada uno diseñado para obtener información del cliente para colaborar con las autoridades de control legal para rastrear y eventualmente evitar cualquier actividad criminal. Estos riesgos crean una posibilidad mayor del uso de las tarjetas prepagadas como un medio para aumentar el lavado de dinero, el financiamiento del terrorismo y otras transacciones ilegales a través del sistema financiero.

Antes de presentar un producto de tarjeta prepagada, las instituciones financieras deberían considerar sus riesgos y crear los controles necesario en sus programas de cumplimiento. Sin el monitoreo adecuado, la institución corre el riesgo de pasar por alto irregularidades tanto en el uso de la tarjeta como en la conducta del cliente que podrían estar asociadas con varios tipos de actividades criminales como el robo de identidad, el fraude con tarjetas de crédito/débito, la evasión o elusión de impuestos, el lavado de dinero y otros, incluidas las actividades vinculadas al financiamiento del terrorismo. La omisión de la identificación adecuada de estos crímenes financieros podría terminar en consecuencias graves, desde sanciones monetarias como resultado de violaciones regulatorias, hasta importantes pérdidas financieras para la institución financiera emisora. Las instituciones financieras que estén considerando ofrecer productos de tarjetas prepagadas deberían analizar la siguiente guía de FinCEN:

- Crear reglas y regulaciones claramente establecidas, como límites importantes en la funcionalidad de la tarjeta para mitigar los riesgos de fraude y lavado de dinero.
- Crear un Programa de Identificación del Cliente (PIC).
- Implementar sistema de monitoreo de fraude y reporte automáticos que evalúen elementos de la información similares a aquellos relevantes para detectar operaciones sospechosas y otras informaciones importantes para la LSB .

> Antes de aceptar solicitudes y abrir cuentas, la institución financiera debe establecer la funcionalidad y los límites de las transacciones de las tarjetas prepagadas

Elaboración de reglas y regulaciones

Antes de aceptar solicitudes y abrir cuentas, la institución financiera debe establecer la funcionalidad y los límites de las transacciones de las tarjetas prepagadas. El establecimiento de estos parámetros puede ser una tarea desafiante al tratar de lograr un equilibrio entre el deseo de atraer clientes nuevos y al mismo tiempo tratar de mitigar el riesgo de que el producto sea utilizado para actividades ilegales. Puede ser difícil satisfacer los pedidos y necesidades del cliente y a la vez asegurar que esas necesidades no creen vulnerabilidades para la institución financiera. Afortunadamente, varias fuentes gubernamentales y otras instituciones financieras emisoras han publicado información sobre la elaboración de un programa sólido para las tarjetas prepagadas para guiar a otras instituciones.

Una de las recomendaciones de FinCEN es someter a todos los productos de tarjetas prepagadas a límites que sean visibles claramente en el producto. Entre los ejemplos de estos límites se incluye un límite de carga, un monto total máximo y un límite en la extracción de dinero en efectivo. FinCEN sugiere que estos límites no deberían exceder los US$1.000 — un monto elegido por varias razones, incluidas las conclusiones de investigaciones realizadas por la industria para las cargas promedio y máxima inicial y la consistencia en los montos mínimos fijados para otras categorías de Negocios de Servicios Monetarios. El monto máximo de US$1.000 también ha demostrado ser la información de mayor utilidad para las autoridades de control legal y sus investigaciones de crímenes financieros. Además, la suma de US$1.000 pareciera ser razonable y ser un monto suficiente para cubrir las necesidades del consumidor y a la vez ayudar a mantener bajos los riesgos del producto.[3] (Ibid)

Es importante señalar que estas limitaciones no pueden aplicarse a todos; por ende, son necesarias algunas excepciones. Cuando se trate de agencias gubernamentales u otros empleadores verificables que emiten depósitos directos que exceden los US$1.000, las instituciones financieras decidirán si establecen parámetros adicionales que se adapten a esos clientes específicos.

Creación de un Programa de Identificación del Cliente (PIC)

Un paso vital en la creación de un programa de tarjetas prepagadas eficiente y seguro es implementar un Programa de Identificación del Cliente (PIC) que obtenga la información requerida y verifique razonablemente a los solicitantes, antes de emitir la tarjeta. Al obtener detalles suficientes sobre la identificación del cliente e implementar un sistema riguroso para verificar esa información del cliente, las instituciones financieras pueden reducir el factor de anonimato vinculado con las tarjetas prepagadas. El PIC debe incluir la obtención de los elementos requeridos de la información, como el nombre del cliente, fecha de nacimiento, domicilio real y número de identificación emitido por el gobierno, y a la vez asegurar que las medidas tomadas para verificar la identidad del solicitante estén basadas en el riesgo y sean razonables. Si la institución financiera utiliza un programa de software para asistir en la verificación, la institución debe asegurarse que el mismo esté actualizado y sea comparable a los

[3] Departamento del Tesoro de los EE.UU, Red de Control de Crímenes Financieros. (2010). Modificación de la ley de secreto bancario (31 CFR Parte 103). Washington, DC: Obtenida de http://www <http://www/>. fincen.gov/statutes_regs/frn/pdf/Prepaid%20Access%20NPRM.pdf <http://fincen.gov/statutes_regs/frn/pdf/Prepaid%20Access%20NPRM.pdf>

estándares de la industria. Deberían elaborarse controles y monitoreo para la autenticación de rutina de la validación programas de software correspondientes para garantizar su eficacia.

Un PIC altamente efectivo es fundamental para el proceso de conozca a su cliente y es un factor importante para cumplir con las expectativas regulatorias sobre un programa de apertura de cuenta de tarjeta prepagada. Además, durante la verificación y aceptación del cliente, las posibilidades de una detección inicial y prevención de fraude y otros delitos relacionados aumentan exponencialmente. La identificación del fraude y otros delitos en la etapa de aceptación del cliente ayuda a administrar los riesgos de anonimato del cliente, creando a su vez un programa de cumplimiento general de tarjetas prepagadas más sólido.

Además de obtener y verificar la información del cliente, la institución financiera participante debe tener un proceso adecuado de conservación de la información del cliente. Además de las obligaciones de conservación establecidas por FinCEN, el mantenimiento de un registro de la información de los clientes también puede ayudar a mejorar el programa vigente creando un precedente, o línea inicial para futuras transacciones dudosas. Más aún, esta información también podría ayudar a las autoridades de control legal en la investigación de cualquier asunto criminal que pudiere surgir de la(s) cuenta(s) de tarjetas prepagadas.

Implementación de sistemas de monitoreo y reporte

Además de tener un PIC efectivo, deben tomarse medidas adicionales para mitigar aún más los intentos de fraude antes y después de la apertura de la cuenta. Estas medidas adicionales incluyen la implementación de sistemas de monitoreo y reporte sólidos desarrollados para generar señales de alerta o anomalías en el uso de la tarjeta prepagada. El monitoreo de las cuentas en la etapa de solicitud es fundamental para detectar y evitar varios tipos de fraude y actividades que generen problemas. Un ejemplo de un escenario de monitoreo en la etapa de solicitud incluye el monitoreo de la dirección de Protocolo de Internet (Internet Protocol, o IP, por sus siglas en inglés) para aquellos productos que permiten aplicaciones en línea. Si bien los canales de aplicaciones en línea pueden crear un mayor volumen de cuentas nuevas, este canal también genera más oportunidades para identificar a ladrones, defraudadores y sus actividades ilícitas. La aplicación de procesos de aplicación en línea deja poco espacio para la verificación directa del cliente, las instituciones financieras deberían considerar la aplicación de indicadores de actividad sospechosa (SAIs, por sus siglas en inglés) adaptados especialmente, como por ejemplo, la generación de señales de alerta sobre las aplicaciones de varias tarjetas realizadas desde la misma dirección IP.

La identificación de números telefónicos o direcciones iguales o comunes a través del monitoreo de la información en la solicitud también puede indicar que defraudadores están queriendo obtener el producto de tarjeta prepagada para cometer sus actividades ilícitas. Un ejemplo de este tipo de monitoreo incluye los casos en que el solicitante (o varios solicitantes) utilizan el mismo número telefónico y dirección para abrir varias cuentas simultáneamente. Los solicitantes que muestran este tipo de conducta podrían estar tratando de explotar sus procedimientos de incorporación de clientes, la funcionalidad de la tarjeta o podrían estar usando fondos ilegítimos para abrir estas cuentas.

El monitoreo de la actividad de la tarjeta prepagada después de la activación de la cuenta debería reflejar los métodos utilizados para identificar y detectar transacciones sospechosas sobre tarjetas de débito y crédito regulares. Deberían elaborarse los SAIs adecuados, y el monitoreo periódico del portafolio que evalúe estos indicadores debería realizarse para administrar eficientemente el riesgo de las tarjetas. Los ejemplos de SAIs que podrían implementarse incluyen: monitoreo de carga máxima de efectivo y de extracción de efectivo, transacciones en lugares de alto riesgo, carga acumulada en un determinado período de tiempo, y el monitoreo de compras. Cuando se consideren los límites en los SAIs para la detección inicial, deben analizarse los límites de las operaciones de la tarjeta. A menudo el individuo o grupos que usen estos productos operarán justo por debajo de los límites máximos permitidos en un esfuerzo por evitar la detección. Dependiendo de las necesidades y vulnerabilidades de la institución financiera, la revisión periódica mencionada podría ser segmentada en períodos diarios, semanales o mensuales.

Deberían elaborarse controles y monitoreo para la autenticación de rutina de la validación programas de software correspondientes para garantizar su eficacia

Haciendo componendas

Como se indicó anteriormente, el crecimiento de las tarjetas prepagadas no muestra ningún signo de disminución y pareciera que las tarjetas prepagadas han encontrado un lugar dentro del sistema financiero. Las instituciones financieras que investiguen la factibilidad de iniciar un programa de tarjetas prepagadas tienen muchos elementos a tener en cuenta al preparar las bases de su programa. Si bien la rentabilidad potencial de las tarjetas prepagadas las hace aparecer atractivas, los riesgos pueden ser importantes y pueden afectar negativamente a la institución financiera. Estos riesgos pueden evitarse estableciendo un marco de control de cumplimiento adecuado basado en el riesgo. Las políticas que incluyan funcionalidad y límites sensatos a la tarjeta, un PIC efectivo, el monitoreo de la cuenta antes de la activación, y el monitoreo posterior a la activación pueden ayudar a disminuir los riesgos potenciales asociados con este producto, y pueden llevar a un programa de tarjetas prepagadas seguro y próspero.

Kevin Nash CAMS, CFE, CIPP, gerente sr, Investigaciones ALD, Capital One Financial, Richmond, VA, EE.UU., kevin.nash@capitalone.com

Dorina Vornicescu, Investigadora AML, Capital One Financial, Richmond, Virginia, EE.UU. dorina.vornicescu@capitalone.com

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

ACAMS Chapters

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

What are the benefits of joining?

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

ACAMS has chapters throughout the world.

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

Visit us at:

www.acams.org/ACAMS/ACAMS/Communities/Chapters

ACAMS New York Chapter

ACAMS Boston Chapter

ACAMS Chicago Chapter

ACAMS Carolinas Chapter

ACAMS US Capital Chapter

Association of Certified Anti-Money Laundering Specialists ACAMS Australasian Chapter

ACAMS Canada Chapter

ACAMS Northern California Chapter

ACAMS South Florida Chapter

ACAMS Southern California Chapter

ACAMS Nigeria Chapter

ACAMS Richmond Chapter

ACAMS South Africa Chapter

Abordando los desafíos del cumplimiento ALD de las alternativas de pago emergentes:

Siga el camino de ladrillos amarillos (de oro) hacia las monedas digitales

PARTE I

Los emprendedores con iniciativa armados con tecnologías de evolución rápida están cambiando para siempre la manera en cómo realizamos nuestras transacciones financieras. Ellos también están aportando incontables noches de insomnio de una cantidad cada vez mayor de personal de cumplimiento antilavado de dinero (ALD).

> Criminales — que siempre están buscando los últimos y mejores mecanismos de pago para facilitar sus esquemas fraudulentos

Sea que se trate de compra de productos, pago de cuentas o transferencia de dinero de persona a persona utilizando una tarjeta prepagada, un teléfono móvil o Internet, en los últimos años han surgido nuevas alternativas de pago que funcionan a velocidades tan rápidas que la mente casi no puede procesarlas — tanto dentro y mucho más allá de las fronteras de las instituciones financieras reguladas tradicionalmente.

Estas innovaciones de pago comparten un tema en común: responden a una incesante de demanda de formas más rápidas, más seguras y más costo-efectivas de realizar transacciones comerciales y transferir valor. Tampoco tienen respeto por los husos horarios o las fronteras geográficas. ¡Y no dañan el medio ambiente!

Al mismo tiempo, estas innovaciones ofrecen más oportunidades a los criminales — que siempre están buscando los últimos y mejores mecanismos de pago para facilitar sus esquemas fraudulentos, el lavado de dinero, actividades terroristas y otras actividades criminales.

A su vez, las nuevas alternativas de pago desafían a las autoridades de control legal y a los fiscales que deben (1) utilizar un tiempo y recursos preciosos para aprender cómo funcionan estas alternativas de pago a fin de saber cómo y por qué las utilizan los delincuentes y (2) trabajar con leyes y regulaciones que inevitablemente están por detrás de las innovaciones y el uso de dichas innovaciones que hacen los criminales.

Y en cuanto al profesional de cumplimiento ALD, estas nuevas soluciones de pago pueden contribuir a noches de menos descanso o de insomnio; y pueden causar pesadillas.

Aún cuando la línea de negocios notifique anticipadamente su intención de crear una nueva solución de pago, el profesional de cumplimiento ALD inevitablemente tiene que ponerse al día para entender cómo funciona, cuál es el propósito que se pretende darle, quién se espera que se inscriba en ella y cómo será utilizada efectivamente, sin mencionar cómo será monitoreado el cliente. Conocer la solución antes del lanzamiento puede ser incluso más penoso — mental y físicamente — ya que la solución inevitablemente involucra a socios comerciales no tradicionales y proveedores, es difícil de entender los flujos de pago y sin embargo tienen que establecerse los riesgos de lavado de dinero y financiamiento del terrorismo.

Posiblemente incluso más desafiante para el oficial de cumplimiento es el monitoreo de las cuentas del cliente que muestren fondos transfiriéndose hacia y/o desde un tercero proveedor de pagos. En esos casos, el profesional de cumplimiento ALD probablemente tenga poca o ninguna información sobre la fuente o el destino último de los fondos.

Ingrese Divisas Digitales. Las monedas digitales integran una clase de alternativas de pago innovadoras que fueron destinadas instantáneamente para atraer la atención tanto de los criminales como de los funcionarios del área de control legal cuando hicieron su debut a mediados de la década del '90. Más rápidos, más eficientes, con menores costos, instantáneamente globales y potencialmente anónimos, los sistemas de monedas digitales recurrieron a lo mejor de la teoría monetaria y las tecnologías emergentes para monetizar el valor intrínseco de los metales preciosos para ser utilizados en una economía basada en Internet.

Durante este período, los oficiales de cumplimiento ALD en las instituciones financieras tradicionales (p.e., bancos, firmas de valores, compañías de seguros) tuvieron pocas razones para prestarle mucha atención a estas monedas digitales porque eran utilizadas esencialmente con interacción limitada o nula con dichas instituciones. Sin embargo, a medida que el uso de la moneda digital se extiende y es aceptado en una variedad de instituciones financieras, la necesidad de que los profesionales de cumplimiento ALD conozcan mejor — y no pierdan más el sueño — esta alternativa de pagos se vuelve más acuciante.

El primer paso para poder dormir más es entender qué son las monedas digitales y las diferencias entre las monedas digitales y el grupo de rápida proliferación de "monedas virtuales".

¿Qué son las monedas digitales? El término "moneda digital" es utilizado frecuentemente pero no es definido con frecuencia salvo en el contexto de otros términos como "dinero electrónico", "e-efectivo" o "dinero virtual". El Grupo de Acción Financiera (GAFI) en su reporte publicado en Octubre de 2010 sobre "Lavado de Dinero Utilizando Nuevos Métodos de Pago" (Reporte GAFI 2010) brinda un análisis detallado de cómo funcionan las monedas digitales pero no da una definición específica.[1]

Wikipedia define al término "dinero electrónico" para incluir a las "monedas digitales" entre las otras siete clases de "monedas electrónicas". Un término alternativo utilizado comúnmente es "monedas de oro digitales" o "DGCs", por sus siglas en inglés, que es moneda digital respaldada con oro.

Un término más preciso para describir a la "moneda digital" es la "moneda privada", que es un medio de cambio utilizado por una persona o entidad distinta de un gobierno soberano. Una moneda digital puede o no estar respaldada por un metal precioso o un respaldo de valor similar. Típicamente no es "vendida" directamente por el "emisor" de la moneda. En lugar de ello, un "cambiador de moneda" cambia un "decreto" (p.e., la moneda emitida por un gobierno soberano) por una moneda digital, o viceversa, de la misma manera que una casa de cambio de divisas tradicional cambiaría dólares por euros.

Las monedas digitales pueden ser utilizadas como cualquier moneda — para pagar bienes o servicios — si la persona que provee el bien o el servicio desea aceptar la moneda digital como pago.

Aunque ciertos aspectos de los sistemas de moneda digital pueden variar, comparte algunas características comunes. Un cliente accede a la página web del sistema a través de Internet y abre una cuenta. La cuenta luego recibe fondos a través de un "gasto" de la moneda digital desde otra cuenta que ya tiene dinero digital. Un gasto puede ocurrir cuando el dinero digital es transferido de una cuenta a otra, sea en conexión con la compra o venta

[1]Grupo de Acción Financiera, Lavado de Dinero Utilizando los Nuevos Métodos de Pago (2010), disponible en http://www.fatf-gafi.org/document/2/0,3746,en_32250379_32237202_46705794_1_1_1_1,00.html

de productos o servicios, una simple transferencia de una persona a otra o el cambio por parte de una casa de cambio de una moneda *"decreto" (fiat)* por la moneda digital.

La más Antigua, y probablemente la más conocida, moneda digital es el e-gold. Las monedas digitales que actualmente operan incluyen a GoldMoney, Pecunix y Liberty Reserve.

¿En qué se diferencia la moneda digital de la moneda virtual? El término "moneda digital" a veces es utilizado indistintamente con el término "moneda virtual". Las dos se diferencian en parte por la manera en que se desarrollaron y la forma en que son utilizadas.

"Las monedas virtuales" son emitidas para jugar juegos en los mundos virtuales como Entropia y World of Warcraft. A menudo son conocidas como "fichas". Generalmente son compradas y canjeadas del dueño del mundo virtual o del operador del sitio dentro del mundo virtual. Además, se han desarrollado mercados secundarios para permitir que los jugadores compren y vendan monedas virtuales directamente entre ellos.

Cada vez más, las monedas virtuales también son utilizadas en las redes sociales/de apuestas y se está ampliando el alcance de su utilización. Por ejemplo, Linden Labs, que es propietaria y opera Second Life, vende Dólares Linden que pueden ser utilizados para comprar productos y servicios tanto en el mundo virtual como en el mundo real. De esta manera, parece estar desdibujándose la línea entre las monedas digital y virtual.[2]

La incursión de las monedas virtuales en el mundo real se destacó en 2009 cuando el gobierno chino, al enfrentar el rápido crecimiento del uso de las monedas virtuales en el mundo "real", promulgó un decreto restringiendo el uso de las monedas virtuales al mundo virtual. Adoptando el enfoque opuesto, el gobierno coreano sancionó el uso de monedas virtuales tanto en el mundo virtual como en el mundo real.

La proliferación de las monedas virtuales puede ser atribuida a la facilidad con que puede crearse — al menos 30 compañías comercializan las plataformas tecnológicas para instalar monedas virtuales. Si bien difieren las plataformas de las monedas virtuales y digitales, las monedas virtuales no son inmunes a las clases de abuso criminal que han experimentado las monedas digitales.

¿El desafío del oficial de cumplimiento ALD? Las monedas digitales presentan distintos tipos de desafíos de cumplimiento a las distintas clases de entidades.

Dado que los sistemas de moneda digital operan como sistemas cerrados (p.e., la moneda digital circula solo entre los titulares de cuenta en el sistema), un prestador de servicios o proveedor de moneda digital puede ver todas las transacciones en el sistema. La moneda digital utilizada en una transacción puede ser rastreada a través de múltiples transacciones y múltiples cuentas durante largos períodos de tiempo. Sin embargo, el proveedor de la moneda digital, no necesariamente conocerá la fuente original del *decreto* (fiat) que fue cambiado por la moneda digital o quien recibe el *decreto* (fiat) después del cambio por la moneda digital a menos que actúe como una casa de cambio o haya incluido transparencia en su sistema para permitirle ver esta información.

El cambiador de la moneda digital está en una posición única para ver quién están cambiando *decretos* (fiat) por moneda digital y viceversa. El cambiador sin embargo no tendrá posibilidad de ver la transacción entre las cuentas dentro del sistema.

Es poco probable que una institución financiera tradicional ver algún aspecto de una transacción de moneda digital a menos que sea un proveedor o cambiador de moneda digital, acepte depósitos de moneda digital, utilice moneda digital como forma de moneda en sus actividades comerciales regulares o, posiblemente, preste servicios bancarios al proveedor de moneda digital. Por otro lado, la institución financiera tradicional puede ver las transacciones entre sus clientes y los cambiadores de moneda digital, aunque esas transacciones serán en *decreto* (fiat).

Sin perjuicio de quién ve qué, conocer los riesgos de lavado de dinero y financiamiento del terrorismo presentados por las monedas digitales y la elaboración o mejoramiento del programa de cumplimiento ALD para mitigar dichos riesgos requiere un conocimiento de cómo funcionan las monedas digitales (incluidos sus flujos de transacciones), cómo los criminales han abusado de ellas, los desafíos únicos que presentan para el control legal, cómo están regulados actualmente, y qué medidas pueden tomarse para mitigar los riesgos de lavado de dinero y financiamiento del terrorismo asociados con sus modelos de negocios.

¿Por qué están preocupadas las autoridades de control legal? La Evaluación de Amenaza de Lavado de Dinero de 2005 publicada por los EE.UU. (la Evaluación de Amenaza) analizó 13 métodos de lavado de dinero que involucraban entre otras cosas "nuevos e innovadores servicios de pago en línea", incluidas monedas digitales[3]. Aunque no estaba bien documentado y era de alguna manera complejo, el reporte identificaba a varias vulnerabilidades específicas que podrían hacer que esos servicios fueran objeto de abuso de lavado de dinero y otros objetivos criminales financieros.

> El cambiador de la moneda digital está en una posición única para ver quién están cambiando decretos (fiat) por moneda digital y viceversa

En apariencia y obtenidos en gran parte de los detalles de una investigación en curso en ese momento que involucraba a e-gold Ltd, los servicios de moneda digital "más antiguos y más conocidos", la Evaluación de Amenaza resumió los siguientes elementos de interés:

- *Capacidad de Pago Internacional de Persona a Persona.* La capacidad de transferir valor entre distintas jurisdicciones crea dificultades par alas autoridades de control legal que tratan de ejecutar el control o llevar a cabo acciones legales fuera de sus jurisdicciones.
- *Falta de Identificación y Verificación del Cliente.* La clase de información personal requerida en la apertura de cuenta varía de acuerdo con el proveedor del servicio y muchos carecen de identificación del cliente o conservación de registros efectivas, están "mal equipados" para verificar la identificación del cliente o promueven "abiertamente" pagos anónimos.

[2]A diferencia de las monedas digitales, sin embargo, la responsabilidad financiera precisa plasmada por el dinero virtual a menudo es vaga, ya que el emisor generalmente no tienen activos corrientes reservados específicamente para respaldar o rescatar a la moneda en circulación.
[3]Evaluación Nacional de la Amenaza de Lavado de Dinero en 25, disponible en http://www.ustreas.gov/offices/enforcement/pdf/mlta.pdf.

- *Aceptación de Dinero en Efectivo o Giros de Dinero.* La aceptación de dinero en efectivo y giros de dinero por parte de los cambiadores de moneda facilita las transacciones anónimas y reduce el "rastro de la investigación" de las autoridades de control legal.
- *Métodos múltiples utilizados para transferir el valor.* Dinero en efectivo, giros de dinero, tarjetas de crédito y débito y transferencias electrónicas utilizadas para transferir valor a los cambiadores de moneda. Los fondos son transferidos a los cambiadores globalmente a través de transferencias de dinero.
- *Abusos Criminales.* Utilizados (a) por operadores de esquemas Ponzi, (b) para facilitar remates fraudulentos en Internet, esquemas de inversión, intrusiones en computadoras, y esquemas de fraude con tarjetas de crédito y débito y (c) para lavar los fondos obtenidos en otra actividad criminal generada fuera del sistema.
- *Transacciones sin recursos.* Todas las transacciones son finales, y los clientes no tienen recursos si los criminales toman su dinero digital.
- *Falta de políticas y procedimientos ALD consistentes o confiables.* Debido a la falta de regulaciones claras, especialmente en las distintas jurisdicciones, muchos sistemas de pago en línea no están sujetos a ninguna obligación de conservación de registros, reporte o programas de cumplimiento ALD.

En Junio de 2008, luego de la acusación contra e-gold y poco antes de su condena, el Centro Nacional de Inteligencia sobre Narcóticos del Departamento de Justicia de los EE.UU. (NDIC, por sus siglas en inglés) publicó un informe señalando que las monedas digitales son más convenientes que los otros métodos de transferencias de fondos porque las monedas digitales son fáciles de usar, las transacciones pueden realizarse en cualquier momento sin tener en cuenta los límites geográficos y las transacciones son instantáneas e irreversibles.

Al analizar los temas de interés incluidos en la Evaluación de Amenaza, el NDIC se concentró en cómo los sistemas de moneda digital no regulados o escasamente regulados se autopromueven insistentemente como anónimos y no regulados. Señaló que los usuarios de los sistemas de monedas digitales "pueden fondear anónimamente las cuentas de dinero digital, enviar esos fondos (a veces montos sin límites) a otras cuentas de moneda digital en el mundo, y cambiar efectivamente los fondos por monedas digitales — a menudo eludiendo la supervisión regulatoria de los EE.UU.".[4]

El GAFI publicó un informe similar poco después sobre "Vulnerabilidades del Lavado de Dinero y el Financiamiento del Terrorismo de los Sitios Web Comerciales y los Pagos por Internet".[5] Si bien la sección dedicada a las monedas digitales parece basarse solo en el informe del NDIC y la Evaluación de Amenaza, ofreció un buen resumen de las señales de alerta y otras consideraciones para evaluar los riesgos asociados en general con los pagos en Internet.

¿Los riesgos de lavado de dinero y financiamiento del terrorismo de las monedas digitales son más importantes que los de otras alternativas de pago? Cada nueva innovación de pagos presenta su propio conjunto de oportunidades y riesgos únicos de abuso criminal. Como es de esperar, los criminales son los primeros — o están entre los primeros — en adoptar un nuevo método de pago, poniendo a prueba qué tan rápido, qué tan lejos y cuánto valor puede crearse o transferirse con la menor interferencia posible lo más que se pueda. Dadas las características únicas de las monedas digitales, ¿están sujetas a un mayor abuso criminal que otras alternativas de pago y por ende son más riesgosas que otras alternativas de pago?

Como dato anecdótico, la Evaluación de Amenaza informó que las autoridades de control legal observaron que los sistemas de moneda digital "se han convertido en el mecanismo de pago favorito de aquellos que cometen actividades ilícitas en línea". El informe del NDIC de 2008 indicaba que las monedas digitales son un instrumento ideal de lavado de dinero". Esos comentarios sin embargo no establecen que son más riesgosas que otras alternativas de pago.

La actualización de 2010 del GAFI realizada a su Reporte sobre Nuevos Métodos de Pago de 2006[6] informó en el mismo el análisis de 33 estudios de casos que involucraban a NPMs. Encontró que: "si bien el análisis de los estudios de casos confirma que hasta cierto punto los NPMs son vulnerables al abuso de lavado de dinero y financiamiento de terrorismo, es difícil de evaluar la dimensión de la amenaza". Concluía que los riesgos de lavado de dinero y financiamiento del terrorismo "pueden ser mitigados de manera efectiva por varias contramedidas tomadas por los proveedores de servicios de NPM" y sugería que todos los factores de riesgo y los mitigantes del riesgo pueden ser considerados al evaluar el riesgo general de un NPM.

No obstante, una preocupación subyacente en todos estos informes es la falta general de supervisión regulatoria y de controles con relación a los sistemas de moneda digital. Aunque se han hecho esfuerzos en los EE.UU. para dar alguna guía regulatoria formal para las monedas digitales, la mayoría de los sistemas de moneda digital se encuentran fuera de los EE.UU. y la capacidad de los EE.UU. para llegar a esas operaciones es limitada. El informe del NDIC indicaba que "sería casi imposible legislar controles regulatorios que le permitieran al gobierno de los EE.UU. impedir completamente que monedas digitales localizadas en el extranjero fueran utilizadas en los Estados Unidos porque estos servicios están disponibles en Internet".

La Parte II de este artículo analizará los esfuerzos en los EE.UU. para regular las monedas digitales y qué impacto pueden tener sobre el uso criminal de esos sistemas. Se concentrará en particular en las experiencias de e-gold, el pionero de las monedas digitales, la regulación no legislativa que ha sido elaborada para la industria y las lecciones de e-gold para otras clases de métodos emergentes de pago para todo el personal de cumplimiento ALD.

Carol R. Van Cleef, CAMS, socia, Firma de Abogados Patton Boggs LLP, Washington, D.C., EE.UU., CVanCleef@PattonBoggs.com

[4]Departamento de Justicia de los EE.UU., Centro Nacional de Inteligencia sobre Narcóticos, Lavado de Dinero en Monedas Digitales en 1 (2008), disponible en http://www.justice.gov/ndic/pubs28/28675/28675p.pdf.

[5]Grupo de Acción Financiera, Vulnerabilidades de Lavado de Dinero y Financiamiento del Terrorismo de los sitios de Internet comerciales y los Sistemas de Pago en Internet, (2008), disponible en http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf .

[6]Grupo de Acción Financiera, Reporte sobre Nuevos Métodos de Pago (2008), www.fatf-gafi.org/dataoecd/30/47/37627240.pdf.

Cuándo llamar a las autoridades de control legal

Saber cuándo presentar un Reporte de Transacción en Efectivo (RTE) o qué documentación se requiere para abrir una cuenta nueva está claramente definido por la regulación o política de una compañía. La decisión de cuándo presentar un Reporte de Operación Sospechosa (ROS) es menos clara y depende del conocimiento y experiencia personal del profesional ALD/CFT para determinar cuando algo no está bien. Pero cuando se trata de ir más allá de la presentación de un ROS para contactar directamente a las autoridades de control legal, puede ser un llamado difícil.

Como oficial de cumplimiento, puede tener que lidiar con la pregunta de cuándo tomar contacto con las autoridades de control legal y a qué agencia debería llamar. Los siguientes expertos de control legal ofrecen algunas guías que pueden utilizarse cuando se enfrentan estas preguntas.

Si usted siente que la situación amenaza con producir un daño irreparable, haga el llamado, de acuerdo con Rick Adams, Agente Especial retirado de la División Criminal del IRS. "Llame a las autoridades de control legal si cree que va a ser prejudicial para el banco; perjudicar para un depositante, por ejemplo, titulares de cuenta que transfieren dinero a Nigeria o Canadá porque han sido víctimas de fraude con loterías; o perjudicar a otra persona, como abuso a personas de la tercera edad", dijo Adams. "Si usted cree que la situación puede causar un daño a la sociedad, como una posible actividad terrorista, debería reportarlo inmediatamente".

Antes de hacer el llamado, tómese un tiempo para evaluar el riesgo, aconseja Adams. Si una transacción es solo sospechosa, como un patrón de depósito inusual distinto al de sus clientes conocidos, debería reportarlo en un ROS, pero no debería necesariamente llamar a las autoridades de control legal.

> Antes de hacer el llamado, tómese un tiempo para evaluar el riesgo

"Por ejemplo, si uno de sus clientes tiene una empresa de alquiler de videos y no tiene ninguna actividad sospechosa durante dos años pero ahora tiene un gran ingreso de dinero en efectivo, eso es sospechoso", dijo Adams. "Pero solo porque pudiera ser inusual y sospechoso, la actividad, la actividad no necesariamente pasa a ser ilegítima".

Sin embargo hay veces en que las actividades inusuales pueden convertirse en un patrón de transacciones sospechosas constantes y en aumento. Cuando eso sucede, es el momento de entrar en contacto con las autoridades de control legal, según Al Gillum, CAMS, presidente de Advanced Compliance Technologies, LLC, e inspector postal retirado.

"Fíjese los ROSs que está presentando (sobre una persona o compañía)", dijo Gillum. "Si empieza a ver un patrón durante dos o tres semanas en que los montos en dólares son importantes y la actividad es un proceso constante, es el comento de contactar a las autoridades de control legal. Una regla simple que utilizo es llamar cuando la actividad llega a los US$50.000".

Jerry Loke, Agente retirado del IRS y actualmente miembro del Grupo de Trabajo sobre el Crimen Organizado y Control de Narcóticos de Filadelfia (OCDETF, por sus siglas en inglés), también aconseja sobre el tema. Para las instituciones que no tienen contactos con la comunidad de control legal o para aquel oficial de cumplimiento que no está seguro de si una actividad requiere hacer un llamado a las autoridades de control legal, el llamar a un equipo local de revisión de ROS podría ser una mejor opción.

"En situaciones extremas, como las analizadas anteriormente, las autoridades de control legal deben ser notificadas, pero no hay que aplicar determinados parámetros", dijo Loke. "De lo contrario los llamados podrían ser abrumadores. Muchas de las Oficinas de los Fiscales de los EE.UU. tienen funcionando equipos de revisión de ROS. Ellos revisan semanalmente los ROS y se reúnen una vez al mes para presentar los ROSs ante el equipo de control legal formado por distintas agencias. En situaciones donde no se tiene una relación con un equipo ROS, puede ser mejor comunicarse directamente con la Oficina del Fiscal de los EE.UU.".

¿A quién debería llamar?

Una vez que decide contactar a las autoridades de control legal, la pregunta siguiente es a quién llamar.

Si tiene contactos con el sector de control legal, úselos. Si no los tiene, notifique a la agencia correspondiente según el tipo de delito.

"Determine a qué agencia llamar", dijo Adams. "Si se trata de una actividad terrorista, llame al FBI. Si involucra a drogas, llame al IRS o a la DEA. Si sospecha que hay abuso de personas de la tercera edad, llame a control legal local".

Si no tiene contactos con el área de control legal ahora, desarróllelos. Todo oficial de cumplimiento debería tener varios contactos con funcionarios de control legal, según Gillum. Establezca relaciones con las autoridades de control legal y recurra a ellos. El

trabajo en conjunto con los funcionarios de control legal puede ser un activo valioso para su equipo de cumplimiento.

"El desarrollo de una buena relación con las autoridades de control legal en su área es fundamental", dijo Gillum. "Todo oficial de cumplimiento debería tener un punto de contacto con el control legal. Cuando se encuentra ante una situación en la que no está seguro, llame a sus contactos. Pueden darle ideas sobre el tema y preguntarles qué piensan de la situación".

Los oficiales de cumplimiento deberían desarrollar relaciones Fuertes con las autoridades de control legal tanto a nivel federal como local, dijo el Sargento Jim Cox, CAMS, supervisor de la Unidad Especial de Investigaciones, Narcóticos y Lavado de Dinero del Departamento de Policía del Condado de Fairfax, Virginia.

"Soy un firme partidario de que hay que tener ambas", dijo Cox. "Nosotros recibimos todos los ROS en los que aparece el Condado de Fairfax, pero a veces el ROS no nos llega hasta después de dos años de presentado. Para el momento en que recibimos el ROS, a menudo ya estamos trabajando el caso a partir de información que recibimos de la comunidad. Como somos una agencia de control legal local, conocemos a la comunidad y recibimos mucha información de ella. El ROS es importante y colabora con el caso, pero la información que proviene de la comunidad también es muy importante. Si un cajero nota que una persona viene con frecuencia y visita su caja de seguridad y luego hace un depósito de una suma importante de dinero en efectivo, nos encantaría recibir un llamado sobre eso. Si recibimos la llamada, podemos empezar a trabajar el caso".

Haciendo contacto

Si su lista de contactos de control legal es corta, hay varias maneras de mejorarla. Llame a la policía local y pregunte si tienen una unidad de lavado de dinero o de delitos financieros. Pregunte cuándo se reúnen y asista a las reuniones que hagan. Asista a los eventos sociales y de aprendizaje de capítulo local de ACAMS para conocer a los agentes de control federales y locales. "Vaya a las reuniones y conozca a la gente", indicó Cox. "Luego, ya está, ya tiene sus contactos".

Además, no desaproveche los recursos dentro de su organización. Muchas instituciones financieras y negocios de servicios monetarios tienen agentes de control legal retirados dentro de su personal. Pregúnteles si conocen a alguien y pídanles los nombres de a quiénes puede contactar.

"Hágase amigo de esta gente y converse con ellos de vez en cuando", dijo Cox. "Dígales que ha completado un ROS y pregúnteles qué piensan. Dé ese paso adicional, tome contacto con los funcionarios de control legal y luego déjelos que actúen".

Debbie Hitzeroth, CAMS, USPS oficial de cumplimiento LSB/OFAC, Servicio Postal de los EE.UU., Washington, D.C., EE.UU., deborah.l.hitzeroth@usps.gov

Antes — y Después — De comenzar a conversar con las autoridades de control legal

Información importante para los abogados

Todos reconocen la importancia de cooperar con la comunidad de control legal y valoran cuánto incluso una pequeña porción de información puede brindar el detalle crucial que ayude a resolver un delito o impedir un acto terrorista.

Sin embargo, si usted decide levantar el teléfono y llamar a las autoridades de control legal, querrá asegurarse que no está creando un problema no deseado para su institución — y posiblemente para usted también.

Para obtener asesoramiento interno sobre cómo evitar esas consecuencias, les pedí sus opiniones a dos de mis socios: Ted Planzos quien fue fiscal asistente en el Condado de Bronx, en Nueva York, un fiscal federal especial asistente y al subjefe de la Sección de Crimen Organizado y Fraude del Departamento de Justicia de los EE.UU.; y a Sam Rosenthal, quien fue fiscal federal asistente y dirigió la Sección de Apelaciones Criminales del Departamento de Justicia de los EE.UU. Ted recientemente representó al Pamrapo Savings Bank en su negociación con el Departamento de Justicia y los reguladores federales. Sam ha representado a varios bancos y remesadoras de dinero en procesos criminales ante fiscales federales y estatales.

A continuación detallamos una lista de señaladores que elaboramos para cuando mantenga conversaciones con las autoridades de control legal.

- *Las Circunstancias Determinarán la Situación.* Todos estamos de acuerdo en que sus comunicaciones con las autoridades de control legal dependerán de las circunstancias, incluyendo si usted tiene información sobre un cliente o uno de sus empleados, si una investigación ya ha sido iniciada y cuál es la naturaleza de la información. Por ejemplo, si la información se relaciona con una investigación criminal o un acto terrorista que implique daños a personas o destrucción de propiedad, probablemente se le pedirá que responda con detalles más rápidamente que si la información estuviere vinculada a una violación previa de escasa o ninguna importancia.
- *La Cooperación es la Mejor Política.* Las Guías Federales de Dictado de Sentencias dejan en claro que la cooperación total con las autoridades de control es un factor considerado por los fiscales al acusar a una compañía de lavado de dinero o de complicidad en actividades de lavado de dinero. Si un empleado estuviera involucrado o la institución de alguna manera estuviere implicada en la actividad, la cooperación será un factor importante de mitigación en el juicio y para el juez al dictar sentencia.
- *Usted Puede Tener que Llamar.* Las instituciones financieras deben notificar a las autoridades de control legal telefónicamente si el asunto requiere su inmediata atención (también debería llamar a su regulador). El Manual de Examen LSB/ALD del FFIEC indica: "para los casos en que se requiera la atención inmediata, además de presentar el ROS oportunamente, el banco debe notificar inmediatamente, por teléfono, a una "autoridad de control legal correspondiente" y, si fuere necesario, al principal regulador del banco".
- *Sea Breve.* Ted sugiere que la mejor estrategia es tener una conversación breve. "Usted solo necesita decirles a los investigadores que se ha presentado o se presentará un ROS. Ellos pueden requerir los documentos". Sam señala que "cualquier conversación con las autoridades de control legal es un evento importante sea que usted llame para informar algún tema de interés o preocupación sobre un cliente o un empleado de la institución. Todo lo que diga se convierte en evidencia". Esto significa que la información que usted brinda a las autoridades de control legal en una conversación posiblemente podría ser utilizada contra la institución más adelante.
- *Informe sobre el ROS Si Se Lo Piden Y Ofrézcalo Cuando Corresponda.* Las nuevas regulaciones sobre divulgación de ROSs publicadas en diciembre de 2010 generalmente prohíben la divulgación de

un ROS. Sin embargo, la regulación brinda una importante excepción que le permite a la institución informar a las autoridades de control legal federal, estatal y local informarles que se ha presentado un ROS o los hechos que indiquen la existencia de un ROS siempre que la divulgación no sea realizada a la persona involucrada en la transacción sospechosa. La nueva regulación también le permite a la institución entregar una copia del ROS a las autoridades de control legal.

- *Aún Podría Requerirse Una Orden Judicial.* Las nuevas regulaciones sobre ROS dejan en claro que puede informarse sobre un ROS a las autoridades de control legal sin una orden judicial. Sin embargo, si bien las regulaciones autorizan la divulgación de los hechos subyacentes, con relación las transacciones y los documentos sobre los cuales está fundamentado el ROS, la regulación no parece eliminar la necesidad de una orden judicial en el caso de que las autoridades de control legal requieran la documentación respaldatoria.
- *Tenga Cerca el Número de su Asesor Legal.* Sea que usted tenga asesoramiento legal interno o externo, no dude en consultar con su abogado si tiene alguna duda sobre si debe contactar a las autoridades de control legal o sobre lo que debe decir en la conversación. Por ejemplo, puede considerar consultar con un abogado sobre si se requiere una orden judicial en el supuesto de que las autoridades de control legal soliciten los documentos respaldatorios. Ted y Sam también están de acuerdo en que en ciertas situaciones donde pueda requerir asesoramiento legal, su asesor participe con usted en la conversación. El costo de contar con el asesor legal se compensaría fácilmente que si tuviera que pagar multas o sanciones elevadas si no se toman las medidas adecuadas. ¿El clásico "mejor estar seguro que lamentarlo"?.
- *Por Último Pero No Menos Importante — No Olvide Presentar el ROS.* Si decidió que la situación era lo suficientemente sospechosa como para llamar a las autoridades de control legal, probablemente sería muy difícil argumentar que no era lo suficientemente sospechoso como para presentar un ROS. Si decidió que no era sospechoso cuando llamó a las autoridades de control legal, entonces puede requerirse o no la presentación de un ROS. Si las autoridades de control legal parecen no interesadas o manifiestan explícitamente que el asunto no es sospechoso, usted tiene la opción. Ésta será una decisión. Si las autoridades de control legal indican de alguna manera que la información es de utilidad, o ayudan a confirmar que se está investigando algo o que será utilizado para iniciar una investigación, entonces debería considerar seriamente presentar un ROS.

Estas breves y simples ideas tienen como objetivo ayudarle a mantener las líneas de comunicación abiertas entre su institución y los representantes de la comunidad de control legal y proteger al mismo tiempo los intereses de su institución. Su asesor legal podrá brindarle algunas sugerencias adicionales.

Carol R. Van Cleef, CAMS, socia, Firma de Abogados Patton Boggs LLP, Washington, D.C., EE.UU., CVanCleef@PattonBoggs.com

Reporte de Actividad Sospechosa:
La seguridad de la calidad es fundamental para maximizar el valor del reporte

Reportar actividades sospechosas a las autoridades gubernamentales competentes es una de las maneras más importantes en que las instituciones financieras participan en la lucha contra el lavado de dinero y el financiamiento del terrorismo. Las leyes de la mayoría de los países han asignado ciertas funciones a las instituciones financieras, convirtiéndolas en fuentes vitales de información e inteligencias sobre las actividades financieras sospechosas de sus clientes. El reporte de operación sospechosa (ROS) (en este artículo se utiliza el término ROS, aunque muchas otras jurisdicciones lo denominan de otra manera) representa la transferencia de esta valiosa información a las autoridades de control legal. Si se hace correctamente, se reflejará bien en la institución, demostrando cómo los esfuerzos de diligencia debida sobre el cliente le permitieron identificar la actividad inusual y discernir que era realmente sospechoso y que correspondía ser reportado.

Si embargo, si el reporte no está bien redactado, puede resultar en una falla al transmitir esta información vital. Esto puede reflejarse deficientemente sobre la institución, así también como ser la diferencia para que las autoridades de control legal inicien o no una investigación sobre los sospechosos y ponga fina a cualquier actividad ilegal subyacente. Como indica el Manual de Examen LSB/ALD del FFIEC, "un ROS detallado y complete puede ser la diferencia al determinar si la conducta descrita y su posible naturaleza criminal son claramente conocidas por las autoridades de control legal. Así, una falla o deficiencia en la descripción correcta de los factores que hacen que una transacción o actividad sea sospechosa afecta el objetivo del ROS".

En los Estados Unidos, varios prominentes procedimientos de control legal han criticado a las instituciones financieras por presentar ROSs poco efectivos, tanto en términos de reporte inadecuado como así también por no presentar ROSs en tiempo oportuno. Si bien no todas las jurisdicciones establecen un plazo dentro del cual debe presentarse el reporte de operación sospechosa, cuando más rápido sea transmitida la información a las autoridades competentes, más pronto se pueden tomar las medidas adecuadas para detener las actividades ilegales. Las instituciones financieras deberían tener medios para realizar una revisión de la oportunidad y calidad de los ROSs para demostrar su compromiso con este aspecto crítico de sus programas ALD, así también como de sus esfuerzos generales para combatir el crimen.

¿Qué se entiende por calidad del reporte?

El término calidad ha sido objeto de numerosos documentos de guía publicados por varias agencias regulatorias. Los temas comunes para definir el término calidad incluyen la suficiencia, precisión y oportu-

nidad del reporte. Por lo tanto, ¿qué separa realmente a un ROS simplemente preciso de un ROS de calidad? La precisión de la información en el reporte debería ser considerada como un estándar mínimo. Toda la información que presenta no debería contener ningún error y ser lo más completa posible. Es esencial para quien lo redacta asegurar la precisión y suficiencia de los espacios del reporte antes de realización la presentación formal. La información inexacta podría demorar un caso criminal de control legal por la inhabilidad para identificar al sospechoso o potencial objetivo correctamente. Además, la presentación de un ROS con información incorrecta, como un identificador personal incorrecto, podría hacer que la institución financiera presentar un reporte modificatorio para corregirlo, lo que hace que los recursos no puedan dedicarse al flujo de trabajo corriente para corregir un elemento que debería haber sido evitado inicialmente.

> La presentación de un ROS y la determinación de la actividad sospechosa generalmente son responsabilidad de un grupo de investigaciones

Además de la exactitud de la información, un reporte de calidad debería detallar toda la información disponible desde la perspectiva de la institución financiera y realizar una descripción de manera tal que sea lógica y detallada. La institución financiera conoce una cantidad importante de información sobre el cliente que puede no ser evidente inmediatamente para que el funcionario de control legal pueda investigar al cliente. La persona que prepara el reporte debería ser muy cuidadosa en la redacción de la descripción y describir correctamente a las personas y eventos asociados con la actividad. Otra guía fundamental en la redacción de una descripción estándar debería ser saber: *quién* está realizando la actividad y quién está involucrado en la actividad; cuáles son las transacciones involucradas (incluidos los tipos de transacciones y los montos de las transacciones); *dónde* se realizan las transacciones; *cuándo* se realizaron las transacciones y tal vez lo más importante, *por qué* considera que la actividad es sospechosa. La descripción también debería describir *cómo* ocurrió la actividad sospechosa, mostrando claramente cómo las transacciones o patrones sospechosos fueron cometidos. El redactor debería incluir en la descripción todos los hechos conocidos durante el análisis de la actividad, aún cuando los hechos parezcan ser triviales en su naturaleza.

Desarrollando un proceso de control del calidad

La calidad y la exactitud son la responsabilidad de cualquier que revise un borrador de un ROS antes de realizar la presentación formal del reporte. La presentación de un ROS y la determinación de la actividad sospechosa generalmente son responsabilidad de un grupo de investigaciones. El redactor del reporte tiene una responsabilidad fundamental para asegurar que la información reportada sea exacta y no contenga errores. El redactor también es la persona dentro de la institución que conoce la totalidad de la actividad sospechosa, incluidas las partes relaciones. La institución debería implementar un proceso mediante el cual el líder del equipo o el gerente senior revise los ROSs antes de realizar la presentación. Quien lo revise, que a su vez no está tan familiarizado con la actividad sospechosa como el redactor, puede realizar una investigación independiente del ROS para determinar si es correcta y si explica claramente la actividad sospechosa que está siendo reportada. Aquél que lo revisa, como miembro del grupo de investigaciones, también tiene un interés personal en la precisión y calidad de la información presentada en el borrador del ROS, ya que esto impacta directamente en la productividad de la unidad. Éste es el momento oportuno para realizar cualquier cambio o corregir la información contenida en el borrador. El tomar este paso extra ayudará a prevenir errores en la presentación y a evitar un trabajo adicional por parte de la institución.

Las instituciones financieras pueden llevar la evaluación del ROS a otro nivel mediante la creación de un equipo independiente de analistas de Control de Calidad que revise los ROSs después de la presentación. Si bien puede ser costumbre hacer que las revisiones antes de la presentación sean hechas por los líderes de los equipos o por los gerentes senior dentro de un grupo de investigaciones o de inteligencia financiera centralizado, un Segundo grupo de revisión fuera del grupo de presentación de ROS centralizado es un grupo independiente que puede brindar un gran caudal de información a la gerencia superior. El foco de atención de este grupo secundario es revisar los ROSs presentados y validar la información reportada respecto de la información contenida en los sistemas de clientes y cuentas de la institución.

El grupo independiente de Control de Calidad del ROS puede aplicar sus propios procedimientos y metodología de calificación para evaluar correctamente las presentaciones de ROS realizadas por el grupo o incluso por un individuo. El grupo de Control de Calidad de ROS es un nivel adicional para determinar la precisión, suficiencia y oportunidad del ROS. Dado que la decisión de presentar un ROS es a menudo una determinación subjetiva, el grupo de Control de Calidad de ROS generalmente no está concentrado en la determinación de si se requería la decisión de presentar un ROS o no. Sin embargo, debería considerar analizar las decisiones por parte del grupo de investigaciones en aquellos casos en que determine que no se requiere un ROS para establecer que la unidad de investigaciones esté documentando correctamente estas decisiones.

Tanto el grupo de Control de Calidad de ROS como quienes revisan las investigaciones también pueden dar información sobre algunas tendencias internas en la presentación e identificar patrones en la presentación de los ROSs que pueden ser de importancia para la gerencia superior. Los equipos de revisión también facilitan la identificación de errores específicos por parte de determinados redactores, permitiendo que la institución adapte una actualización de la capacitación para corregir el tema y prevenir errores futuros. El seguimiento de la calidad del ROS por parte de los redactores también puede ser utilizado como barómetro del desempeño de un individuo o de un equipo durante las revisiones de personal programadas regularmente. La función también puede ayudar a resolver temas antes de una auditoria formal o a un examen regulatorio.

Impactos de los ROSs de mala calidad

Existen varias consecuencias importantes derivadas de los ROSs de mala calidad. Si bien la implementación de un proceso de Control de Calidad de ROS conlleva una gran cantidad de recursos cada vez mayor en términos de tiempo de dedicación del

personal, las consecuencias adversas superan los costos que puedan implicar. Los ROSs de mala calidad pueden resultar en revisiones o corrección de las presentaciones ya efectuadas, lo cual, si ocurre frecuentemente, puede terminar en un examen menos satisfactorio por parte de los reguladores, que probablemente verán un proceso con muchas deficiencias. Si bien algunos sistemas pueden tener controles automáticos que evalúan si la información está incluida o no dentro de los campos de reporte requeridos, éstos a menudo no pueden evaluar la calidad o precisión de la información, dos aspectos que pueden llevar a presentaciones modificadas. Como con cualquier examen menos que satisfactoria, la institución deberán gastar una importante cantidad de recursos para corregir la deficiencia — a menudo implementando la función de control de calidad de ROS que debería haberse aplicado. Además, los errores constantes en la presentación de los ROSs pueden resultar en sanciones monetarias por parte de los reguladores, lo que a su vez puede generar un daño reputacional si los acuerdos se hacen públicos.

Sin embargo, fuera del impacto directo sobre la institución, un ROS de baja calidad puede llevar a una demora en la investigación de actividades que pudieren ser potencialmente criminales. Por ejemplo, si una institución no entrega información precisa, podría impedir que las autoridades de control legal investiguen al sospechoso correcto. Si una institución no envía la información correcta de la cuenta, podría resultar en que los funcionarios de control legal emitan una orden judicial pidiendo información incorrecto, lo que a su vez resultaría en una situación embarazosa si la institución devolviera la orden judicial con información de que no existe tal cuenta en sus libros o de que la información no está relacionada con la actividad inusual subyacente. Los funcionarios de control legal a menudo revisarán los ROSs emitidos para determinar si hay bases suficientes para realizar una investigación de cualquier posible actividad criminal. Si el ROS de una institución no incluye una explicación suficiente de porqué la actividad es sospechosa, el área de control legal ni siquiera puede iniciar la investigación. Este último escenario debe ser uno de los resultados más frustrantes de la presentación de ROSs — que todo el esfuerzo de la investigación aplicado por la institución lleve a nada más que nada útil en el sistema, mientras que la actividad criminal continúa su marcha. Además los ROSs de mala calidad también pueden desviar los recursos limitados del sector de control legal haciendo que haga un seguimiento con las instituciones para obtener información que debería haber sido incluida en el reporte original.

Un ROS mal preparado podría producir un impacto en la capacidad de las autoridades de control legal de identificar y rastrear un patrón de actividad de un posible lavador de dinero o un financista del terrorismo. Esto a su vez tiene un impacto sobre el bienestar financiero, así también como sobre la seguridad de la comunidad en la cual presta servicios la institución y donde viven sus clientes y empleados.

Respuestas del control legal

Las agencias de control legal y gubernamentales regulatorias han señalado que la calidad de la información de los ROS ha llevado a la investigación y condena de criminales y cómplices. Para reforzar el punto de que el ROS representa la relación más importante entre el programa ALD de una institución y el control legal, un ROS de calidad muestra claramente a las autoridades de control legal lo que la institución ha observado, porqué es inusual y les da información que necesitan para hacer un seguimiento e investigar más la actividad inusual.

Los funcionarios de control legal generalmente no están tan bien entrenados en el análisis de las transacciones financieras como los investigadores ALD de las instituciones; especialmente en lo que respecta a cómo navegar los sistemas de la institución para seguir el rastro del dinero. Así, es a través del ROS que la institución puede articular el flujo de fondos, que es exactamente lo que las autoridades de control legal necesitan para rastrear la actividad criminal que pueden detectar — y que generalmente es su responsabilidad determinar — los fondos que pueden decomisarles a los criminales.

A lo largo de los años, los investigadores de su institución han recibido numerosos elogios de las autoridades de control legal citando cómo la información que les habían brindado les había permitido a los funcionarios de control legal seguir complicados y sofisticados laberintos de transacciones diseñadas para ocultar el rastro de los fondos y llevar a los delincuentes ante la justicia y decomisar los fondos que podían ser utilizados para compensar a las víctimas de los delitos. De hecho, la cantidad de estos elogios ha aumentado como resultado de la implementación del proceso de Control de Calidad de ROS. Estos halagos han sido un enorme estímulo para la moral de nuestros investigadores, llevando a una mayor productividad, así también como al fortalecimiento de una relación de trabajo más fuerte entre los investigadores de la institución y los funcionarios de control legal.

Las agencias de control legal y gubernamentales regulatorias han señalado que la calidad de la información de los ROS ha llevado a la investigación y condena de criminales y cómplices

Conclusión

El ROS es una de las maneras más importantes en las que el programa ALD de una institución combate realmente los delitos que subyacen al lavado de dinero y el financiamiento del terrorismo. Así, es una de las contribuciones más importantes que las instituciones financieras pueden hacer a las comunidades a las que prestan servicios. Si bien cualquier clase de datos pueden ayudar, la mala calidad de los ROS generalmente no guiará a los investigadores y puede socavar recursos que podrían ser utilizados para perseguir la actividad criminal. Los ROSs de calidad son aquellos que llevarán a mejoras importantes en la forma en que las autoridades de control legal pueden utilizar la información que las instituciones les brindan sobre las actividades sospechosas. Un proceso diseñado para asegurar la calidad en todos los ROS ayuda a maximizar el valor y la utilidad de los ROSs de la institución, demuestra su compromiso para combatir el lavado de dinero y el financiamiento del terrorismo, minimiza la repetición innecesaria del trabajo y crea una asociación fuerte con las autoridades de control legal.

Melissa Morelli, CAMS, vicepresidenta, Bank of America, Charlotte, Carolina del Norte EE.UU.,Melissa.l.morelli@bankofamerica.com

Kevin M. Anderson, CAMS, director, Bank of America, Falls Church, VA, EE.UU., Kevin.m.anderson@bankofamerica.com

Pre-Conference Training: September 18, 2011
Main Conference: September 19-21, 2011

ARIA • LAS VEGAS

ACAMS Members pay only $1245*!

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

ACAMS 10th Annual International

Anti-Money Laundering CONFERENCE

Reserve your seat today!

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




Presented by

Association of Certified Anti-Money Laundering Specialists®

ACAMS®

Register now! * • info@acams.org • +1 305.373.0020

acamsglobal.org

MEDIA PARTNERS: MONEY LAUNDERING.COM COMPLIANCE ADVANTAGE.COM

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

Los inspectores del FFIEC golpean su puerta

Damas y caballeros, permítanme presentarles al Registro Federal (Federal Register). ¿Ya conocen sus increíbles poderes? Si es así, entonces este artículo podría no ser para ustedes. Si, sin embargo, leyeron la misma regulación una y otra vez pero todavía están tratando de saber qué significa, o necesitan entender verdaderamente la intención detrás de una regla en particular, entonces el Registro es su lugar.

Primero déjeme darle alguna información sobre los antecedentes. Un proyecto de ley, como la Ley de Secreto Bancario (LSB), después del proceso de los poderes legislativo y ejecutivo, se convierte en ley o acto. Una ley/acto puede ejecutarse en sí misma, entendiéndose que no se necesitan regulaciones antes de su publicación, o, por el contrario, una ley/acto puede requerir la publicación de regulaciones.

Las regulaciones explican cómo debe ser aplicada o interpretada la ley. Antes de publicar las regulaciones, sin embargo, la agencia responsable o el departamento responsable emitirán propuestas de reglas. Estas propuestas reciben comentarios de los miembros de la industria sobre la que producirá impacto la Ley. La agencia analizará los comentarios, discutirá las razones para la incorporación o rechazo de dichos comentarios y eventualmente publicará las regulaciones finales. Este proceso de dar y recibir entre la industria y la agencia regulatoria es reproducido en el Registro Federal y es este "dar y recibir" lo que puede ser valioso.

A continuación se indica un ejemplo de una ventaja del Registro Federal.

La Sección 5318 (i) de la LSB requiere la diligencia debida par alas Cuentas Bancarias Corresponsales y de Banca Privada de los Estados Unidos Relacionadas con Personas Extranjeras Yendo un poco más allá, la sección 5318(i)(3) establece que … *como mínimo, … la institución financiera tome medidas razonables (A) para determinar la identidad de los dueños nominales y beneficiarios de, y la fuente de los fondos depositados en, dicha cuenta.*

La LSB requiere que se tomen medidas razonables para determinar la fuente de los fondos depositados en una cuenta Bancaria Privada en la que haya Personas Extranjeras. La tarea puede parecer dantes y tal vez imposible cuando se analizan aspectos como el volumen de transacciones en una cuenta y los obstáculos que se presentan para verificar casi cualquier información. Simplemente reformulando la LSB, las Regulaciones, específicamente 31 CFR 103.178 (b)(2), no se llega a comprender totalmente. El Registro Federal, sin embargo, ofrece un lenguaje útil que ayuda a determinar cómo convertir la redacción de la LSB en una realidad comprensible.

"… no esperamos que las instituciones financieras cubiertas, en el curso ordinario, verifiquen la fuente de cada depósito realizado en cada cuenta de banca privada. Sin embargo, deberían monitorear los depósitos y transacciones en la medida que fuere necesario para asegurar que la actividad sea consistente con la información que la institución ha recibido sobre la fuente de los fondos del cliente y con el objetivo indicado y el uso esperado de la cuenta, en la medida que sea necesario para protegerse contra el lavado de dinero, y para reportar cualquier actividad sospechosa". Registro Federal, Vol.71, No.2/Miércoles 4 de Enero de 2006/ Reglas y Regulaciones, Página 509.

Solo después de leer las secciones relevantes del Registro Federal es que se puede empezar a conceptualizar cómo cumplir con la LSB. En esta situación, las instituciones financieras no están obligadas a verificar la fuente de cada depósito — es simple y está claro.

A continuación se indica un "dar y recibir" útil.

La Sección 3518 (i) (3) (A) de la LSB requiere que las instituciones financieras (A) determinen la identidad de los dueños nominales y beneficiarios. En las Regulaciones se entiende que un dueño beneficiario de una cuenta es *un individuo que tiene un nivel de control sobre, o el derecho sobre, los fondos o bienes en la cuenta que, como resultado práctico, le permite al individuo, directa o indirectamente, controlar, administrar o dirigir la cuenta. La capacidad para fondear la cuenta o el derecho a los fondos de la cuenta solamente, sin embargo, sin alguna autoridad correspondiente para controlar, administrar o dirigir la cuenta (como en el caso de un beneficiario menor de edad), no hace que el individuo sea un dueño beneficiario.* 31 CFR §103.175 (b).

La regla propuesta originalmente era diferente. Utilizaba el término Interés de Dueño Beneficiario *(Beneficial Owner Interest)* lo que implicaba que casi cualquiera que tuviera acceso a la cuenta cayera dentro de

la obligación de "identificación". También existe un monto mínimo en dólares del interés, pero eso no es importante para este análisis. Los problemas con la regla propuesta originalmente fueron presentados a través de varios comentarios.

"…las Asociaciones creen que la definición de "interés de dueño beneficiario" es demasiado amplia. Un enfoque posible podría ser que la regla final no tratara de definir el "interés de dueño beneficiario" con terminología general, sino permitir que las instituciones financieras cubiertas determinen qué personas, en determinadas circunstancias, deberían ser consideradas como que cumplen el requisito de la propiedad beneficiaria. El requisito de la propiedad beneficiaria podría ser determinado por referencia por el nivel de propiedad que, como asunto práctico, equivale al control sobre o el derecho a la cuenta …" *Carta Conjunta de: Asociación de Finanzas y Comercio de Valores de la Asociación de Banqueros Estadounidenses y la Mesa Redonda sobre Servicios Financieros al Comercio de la Asociación de la Industria de Futuros — 1ro. de Julio de 2001.*

Los argumentos fueron persuasivos y la definición fue limitada. El Registro continúa explicando, *"La Regla también deberían darles a las instituciones financieras cubiertas un estándar factible para evaluar la propiedad beneficiaria de las cuentas bancarias privada, permitiéndoles así a las instituciones financieras cubiertas concentrar sus esfuerzos de diligencia debida en un enfoque basado en el resigo de esas cuentas e individuos que presentan un mayor riesgo de lavado de dinero". Registro Federal /Vol.71, No. 2/Miércoles 4 de Enero de 2006, Reglas y Regulaciones. P 505.*

Al final, lo que hay que recordar es concentrar sus esfuerzos de diligencia debida según el riesgo que esas cuentas e individuos presentan de un mayor riesgo de lavado de dinero. ¡Muchas gracias Registro Federal!

Para ser claros, el Registro Federal no es el único lugar para tener una guía. El manual del FFIEC también ofrece una impresionante cantidad de información. Recuerde, sin embargo, que los escritores del Manual del FFIEC revisan y son convencidos por los contenidos del Registro. La discusión sobre la "fuente de los fondos" mencionada anteriormente es un buen ejemplo. La guía del FFIEC es muy similar a lo que está escrito en el Registro. Vea la página 132 del Manual del FFIEC 2010.

Así, cuando lo único que importa es tener un claro entendimiento de la LSB, vaya a http://www.regulations.gov o http://www.fincen.gov . Ambos son sitios que se pueden navegar fácilmente y que brindan acceso a la LSB y las Regulaciones.

Michael Kneis, CAMS, HIFCA, El Dorado Task Force/ HIDTA, Nueva York, NY, EE.UU., mkneis@nynjhidta.org

¿Viendo en monocromo?

He sido bendecido a lo largo de mis 38 años de carrera profesional al estar asociado con verdaderos excelentes profesionales. Pasé 31 años en la función gubernamental, 28 con la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés). La integridad y dedicación que encontré entre mis colegas de control legal fue digna de mención. Yo estaba extremadamente orgulloso de mis amistades y asociaciones. Durante los últimos siete años como consultor trabajando con especialistas en cumplimiento y fraude, he tenido el privilegio de observar los mismos niveles de integridad y dedicación. También estoy orgulloso de las amistades y asociaciones que he desarrollado en el sector privado.

La principal diferencia entre mis colegas de control legal y del sector privado es la perspectiva. No mucha gente reconoce este importante hecho. Tanto mis contemporáneos de control legal como del sector privado entienden la importancia de trabajar juntos unos con otros. Desafortunadamente, las asociaciones exitosas han sido aisladas y no sistemáticas y sustentables. Una razón para ello es la diferencia de perspectivas.

Muchos de los individuos con los que tuve el honor de trabajar en conjunto en el sector de control legal y el sector privado son pensadores innovadores. Sin embargo, en la mayoría de los casos, no han podido realizar la innovación institucional. El control legal y las instituciones del sector privado tienden a operar en sus zonas seguras, y frecuentemente, la innovación queda fuera de la zona de seguridad institucional. Como resultado de ello, hay muy poco incentivo para elaborar técnicas innovadores para luchar contra el fraude y el lavado de dinero.

Esto me trae al punto central de este artículo: perspectivas, asociaciones e innovación.

Introducción

Cuando se trata de fraude y de lavado de dinero, los malos no se ven enmarcados por los límites. Esto les brinda la oportunidad de ser proactivos e imaginativos en respaldo de sus actividades ilícitas. De hecho, cuanto más proactivos e innovadores son los malos, mayores incentivos obtienen. Por el contrario, las autoridades de control legal y el sector de servicios financieros están con frecuencia limitados por la burocracia y la renuencia a implementar cambios. Las regulaciones, las consideraciones sobre la privacidad, las políticas, procedimientos, restricciones presupuestarias y una gran cantidad de otros factores a menudo son impedimentos para medidas proactivas y nuevas ideas y pensamientos. Las regulaciones son tales que el monitoreo reactivo de las transacciones y la detección del fraude en el sector de servicios financieros es la norma aceptada. Existe poco incentivo para la innovación. En consecuencia, los malos tienen una ventaja importante.

Como hemos visto en los últimos años, los fraudes corporativos, los fraudes con inversiones y los fraudes hipotecarios han devastado a nuestra economía. Hay que agregar a eso el flujo constante de fraude con cheques, fraude con préstamos y fraude con tarjetas de crédito, sin mencionar el fraude con el seguro de salud y otros delitos, y nuestros problemas económicos están significativamente agravados. La única constante en los diversos esquemas de fraude que hemos experimentado es la necesidad constante de lavar estos fondos derivados de actividades criminales. Los puntos en común entre el fraude y el lavado de dinero deberían ser el punto central para la prevención y la disuasión.

Ha llegado el momento de quitarles la ventaja a los malos de una manera sustentable y significativa. Para lograr esto, las autoridades de control legal y el sector de servicios financieros primero deben entender verdaderamente el significado de tres palabras: perspectivas, asociaciones e innovación.

Perspectivas

En muchas de las presentaciones de capacitación que he dado desde que me retiré del FBI, he comentado que cuando me retiré y me convertí en consultor, creía que sabía todo lo que necesitaba saber sobre el antilavado de dinero (ALD) bancario, el cumplimiento sobre fraude y las investigaciones. Lo que me di cuenta en un instante fue lo poco que conocía realmente sobre el cumplimiento ALD y la función de investigación. No se trataba de no saber, se trataba de no entender el cumplimiento y la perspectiva de fraude desde la institución financiera. Esa fue una experiencia humillante y educativa. Durante los últimos siete años, he trabajado mucho para entender y apreciar la perspectiva de la institución financiera. Para beneficio de mis amigos de control legal, si yo hubiera sabido entonces (cuando estaba en la actividad de control legal) lo que sé ahora, hubiera sido peligroso. Aliento a mis colegas de control legal a que aprendan de mi experiencia y a que miren más allá de sus perspectivas cuando traten con el sector privado.

La realidad es que muchos de los oficiales de control legal no entienden la perspectiva de un especialista en cumplimiento o fraude bancario. De la misma manera, muchos especialistas en cumplimiento o fraude bancario no entienden la perspectiva del oficial de control legal. El primer paso para llegar a un trabajo en conjunto sustentable y positive es que ambos lados entiendan y respeten las diferencias que existan en las perspectivas.

La principal diferencia en las perspectivas es que el control legal es dirigido por investigadores criminales. Ellos deben concentrarse en obtener evidencias para sustentar los enjuiciamientos criminales. Los investigadores de bancos se concentran en la identificación y reporte de actividades sospechosa. Estos dos enfoques parecerían incompatibles; sin embargo entre los funcionarios de control legal y los bancos están los reguladores. Sin querer culpar a nadie, el sistema regulatorio es tal que los bancos tienen que satisfacer a los reguladores antes de tener que respaldar la actividad de control legal. Aquí es donde existe la mayor presión para entender la perspectiva. El control legal se concentra en su caso criminal. Generalmente no entienden el dilema de los bancos de tener que satisfacer a los reguladores cunado hay malhechores que tienen que ir a la cárcel. Mientras tanto, los bancos no necesariamente están preocupados por si los malos tienen que ir a prisión. Ellos están preocupados por sacar a los malos fuera de sus bancos y por cómo responderán los reguladores. Para agravar el problema está el hecho de que aunque las regulaciones y leyes están escritas claramente, su implementación e interpretación no es clara y es subjetiva.

El control legal y las instituciones financieras deben solucionar el conflicto en sus respectivas perspectivas y entender que cada uno tiene información que sería muy beneficiosa para el otro. El control legal tiene información de investigaciones e inteligencia sobre los esquemas y tendencias. Con frecuencia escucho quejas y frustración expresadas por los especialistas en cumplimiento bancario e investigaciones de que los funcionarios de control legal no comparten esa información. Por el contrario, los bancos tienen un archive increíble de información e inteligencia financiera que ayudaría muchísimo en las investigaciones criminales si el control legal supiera de su existencia o dónde obtenerla.

El control legal y las instituciones financieras deben ponerse de acuerdo sobre las perspectivas. Una vez logrado eso, se establecerán bases para trabajos en conjunto mucho más productivo. Esas asociaciones estarán mejor posicionadas por ser sustentables y coherentes.

Asociaciones

Ha habido una gran cantidad de asociaciones públicas y privadas que han tenido éxito. La mayoría de éstas han sido a nivel local o no han sido especializadas. Tenemos que desarrollar asociaciones más sólidas a nivel general y, más específicamente, a nivel nacional. El punto inicial debería ser con la comprensión de que el control legal y las instituciones financieras comparten la responsabilidad mutual para proteger a nuestro sistema financiero y a sus clientes frente al fraude y el lavado de dinero.

Una forma de lograr esto es desarrollar asociaciones específicas de acuerdo con el tipo de delito. Al hacerlo, el control legal debería elaborar tipologías de casos específicos de acuerdo con el problema criminal y de acuerdo a cómo las finanzas de la actividad

criminal fluyen a través de las instituciones financieras. Al compartir estas tipologías de casos y la información del análisis de las tendencias con el sector privado, el control legal le permitirá al sector privado identificar más efectiva y eficientemente y reportar las actividades sospechosas. Al hacerlo, ambas partes se benefician. El control legal prepara la evidencia para sostener los juicios criminales y/o, el decomiso y recupero de bienes. Las instituciones financieras a su vez reducirán el riesgo institucional.

Hay un muy buen ejemplo de la asociación pública-privada generada por un problema criminal específico y las tipologías. Fue iniciada por JPMorgan Chase (JPMC) bajo la dirección de William Langford. En 2009, el área ALD Corporativa de JPMC creó un equipo dedicado a identificar y evaluar los riesgos inmediatos y estratégicos de JPMC. Este destacado equipo desarrolló con entusiasmo un enfoque basado en temas mediante el cual identificaron problemas delictivos específicos que les presentaban riesgos significativos. En 2010, JPMC identificó al tráfico de personas como un problema delictivo importante y un vehículo para el riesgo institucional. En general, el proyecto elaboró una tipología basada en los modelos de vigilancia y el entrenamiento del investigador para permitirle identificar mejor el posible tráfico de personas. El equipo del JPMC de dedicados profesionales de cumplimiento y de investigación desarrolló meticulosamente tipologías que les permitieron identificar transacciones asociadas con el tráfico de personas.

El siguiente paso fue desarrollar canales activos para coordinar con las agencias de control legal apropiadas, especialmente aquellas dedicadas específicamente al tráfico de personas. William y su equipo formaron una excelente asociación de trabajo con la oficina de Control de Inmigración y Aduanas (ICE, por sus siglas en inglés), la cual tiene un dedicado grupo de agentes asignado a la investigación del tráfico de personas. A través del intercambio mutuo de información, el JPMC pudo identificar tipologías adicionales mientras que la ICE pudo obtener evidencia para fundamentar juicios criminales.

El tráfico de personas es un problema delictivo atroz. La valiosa asociación formada por el JPMC e ICE ha comenzado a crecer. En Septiembre de 2010, durante la Conferencia Anual de ACAMS, el vicepresidente ejecutivo de ACAMS, John Byrne, organizó una reunión informal, extraoficial, entre representantes de control legal y miembros de la Junta Asesora de ACAMS para analizar cómo podría ACAMS facilitar la asociación entre el control legal y el sector de servicios financieros. Entre algunos de los promisorios resultados de esa reunión, se realizó posteriormente una reunión en Washington, D.C., entre Byrne, el presidente de la junta asesora Rick Small, el miembro de la junta William Langford y ejecutivos senior en ICE. Uno de los temas fue el tráfico de personas.

A causa del devastador impacto de este problema delictivo sobre sus víctimas, ACAMS ha creado un Grupo de Trabajo sobre Tráfico de Personas, presidido por Langford. Esta iniciativa brindará una plataforma para el trabajo en conjunto de los sectores público y privado iniciado por JPMC con ICE para que crezca y sea más sostenible. En respaldo de este esfuerzo, el 13 de Enero de 2011, ACAMS organizó un webseminario de capacitación sobre tráfico de personas. Byrne fue el moderador junto con la agente de ICE Angie Salazar, quienes ofrecieron una apasionante sesión de capacitación. La educación y la capacitación promueven la concientización, lo que frecuentemente lleva a la acción.

Al aplicar el enfoque basado en los temas, el JPMC no adoptó un marco de monitoreo de transacciones tradicional o reactivo. Langford y su equipo adoptaron un enfoque innovador y proactivo ante los desafiantes problemas delictivos. Debe señalarse que el JPMC no está solo en la elaboración de enfoques innovadores para identificar y reportar actividades sospechosas. El JPMC representa solo un ejemplo de cómo ciertas instituciones financieras están gravitando en torno al uso de mecanismos más proactivos.

Innovación

El equipo de Langford realizó una amplia investigación para crear tipologías. Se basaron en la extracción y en el desarrollo de un modelo específico proactivo. Al ser proactivo y estar focalizado, el JPMC identificó más efectiva y eficientemente las actividades sospechosas consistentes con el tráfico de personas. La metodología desarrollada por el JPMC debería servir como modelo para futuros modelos de monitoreo de transacciones.

La industria debe ser menos predecible en el monitoreo de transacciones y más específica y proactiva. Tiene que haber un equilibrio entre el monitoreo de transacciones tradicional reactivo y el monitoreo específico proactivo de determinada actividad. Un enfoque equilibrado entre el monitoreo reactivo y el proactivo haría que "los malos" se mantuvieran alejados en sus esfuerzos por explotar áreas de vulnerabilidad de riesgo.

La industria debe ser menos predecible en el monitoreo de transacciones y más específica y proactiva

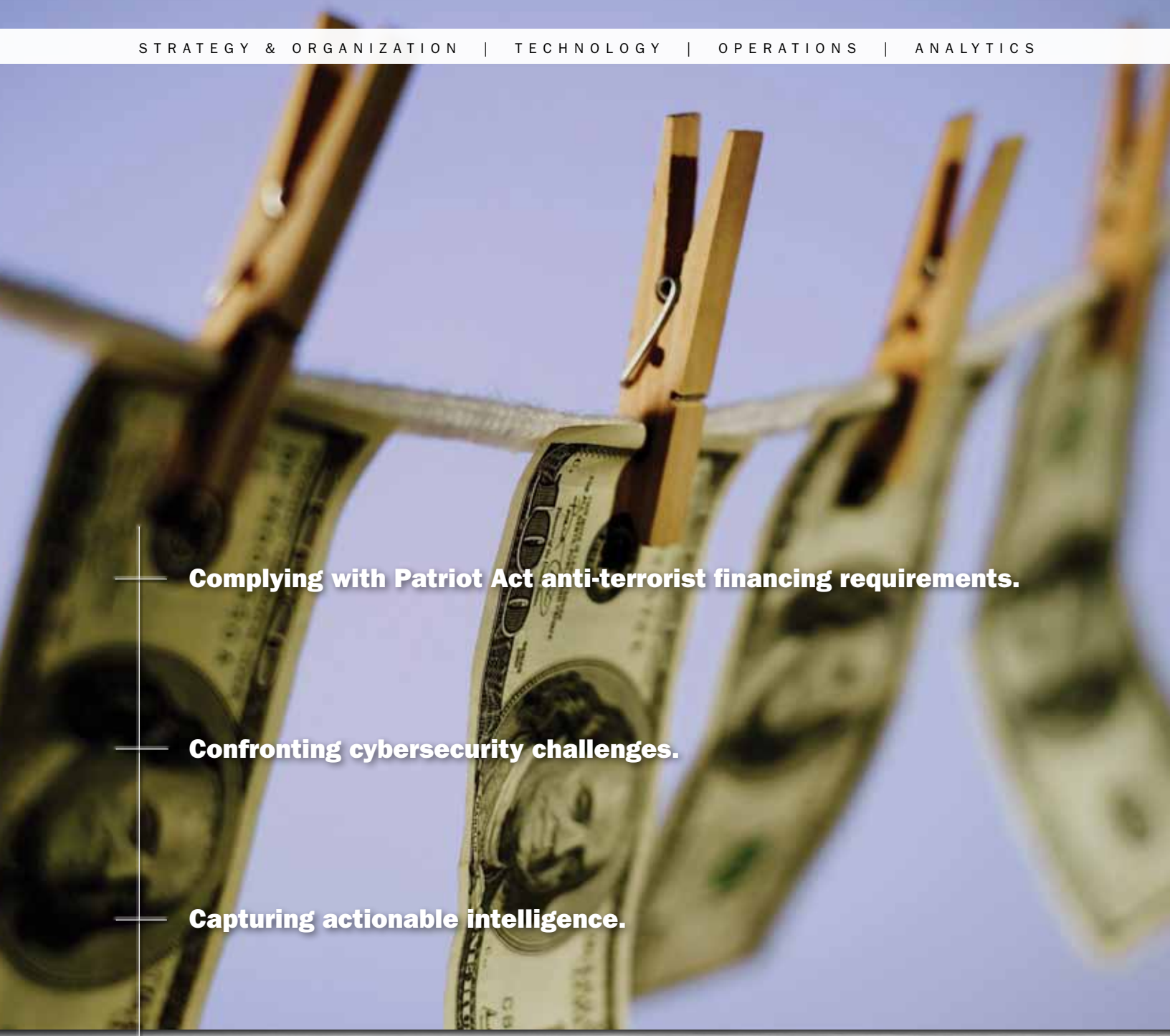
Un incentivo para esto es el desafío de avanzar con este enfoque. El incentivo para el JPMC fue hacer lo correcto. En términos de incentivos tangibles para que las instituciones financieras implementen tipologías y metodologías similares es, no hay mucho sobre el tema. Aquí es donde los reguladores podrían ser un factor. Si hubiere un incentivo regulatorio para desarrollar tipologías y técnicas proactivas de monitoreo de un problema criminal específico, habría más instituciones financieras inclinadas a elaborar programas similares al del JPMC. Esto incrementaría significativamente la consecuente generación de más reportes de actividad sospechosa.

JPMC ha aplicado el enfoque según los temas a otros problemas criminales importantes. Esperemos, en la medida que tenga contacto con otras agencias de control adecuadas para trabajar en conjunto, que esas agencias respondan tan bien como lo hizo la ICE con relación al tráfico de personas. El desarrollo de trabajos en conjunto significativos y sustentables entre los sectores público y privado es la mejor manera de eliminar las ventajas que pudieren aprovechar quienes realizan actividades indebidas.

Conclusión

Dado que los malos no están limitados por las fronteras, cuando se trata de fraude y lavado de dinero, corresponde que el control legal y el sector de servicios financieras compartan la responsabilidad de contener e interrumpir la actividad criminal. Cuando más proactivos y coordinados estén el control legal y la industria, mayor probabilidad habrá de detener a quienes realizan actividades indebidas. La combinación de perspectivas, trabajos en conjunto e innovación brindará el marco necesario para frenar la marea del fraude y el lavado de dinero.

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



Complying with Patriot Act anti-terrorist financing requirements.

Confronting cybersecurity challenges.

Capturing actionable intelligence.

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

Ready for what's next. www.boozallen.com/fas

Booz | Allen | Hamilton

strategy and technology consultants

Evaluaciones de riesgo ALD

– Conceptos y metodologías para comprender cabalmente el riesgo de una institución financiera

El Lavado de Dinero (LD) y el Financiamiento del Terrorismo (FT) son temas globales que atraviesan cada una y todas las fronteras con un gran impacto sobre el sector de servicios financieros. ¿Conoce y comprende el impacto sobre su institución financiera? ¿Puede explicar dónde yace su riesgo LD y FT? Los esfuerzos internacionales para mitigarlos han llevado a cabo esfuerzos para interceptar y combatir tanto la actividad de LD como de FT. Las Recomendaciones del Grupo de Acción Financiera (GAFI) se han trasladado a las Unidades de Inteligencia Financiera de los países, como AUSTRAC, FINTRAC, FIC, JFIU, y FinCEN, por nombrar a algunas. Estas recomendaciones abarcan las expectativas de lo que un programa antilavado de dinero (ALD)/contra el financiamiento del terrorismo (CFT) debería aplicar. Además, la Nota Interpretativa del GAFI sobre el Enfoque Basado en el Riesgo (IN-RBA, por sus siglas en inglés) requiere que las instituciones financieras realicen Evaluaciones de Riesgo ALD/CFT. Al evaluar el riesgo de una institución financiera, estas recomendaciones deberían ser aplicadas y el riesgo evaluado de manera acorde. Dentro de los Estados Unidos, la guía sobre las evaluaciones de riesgo son dadas mediante el Manual de Examen LSB/ALD del Consejo Federal de Examen de Instituciones Financieras (FFIEC, por sus siglas en inglés). Más aún, las instituciones financieras deberían seguir las guías ofrecidas por la UIF, el regulador o el ministerio de finanzas de sus países.

La evaluación del riesgo ALD y CTF debería ser la fuerza generadora del programa de cumplimiento ALD/CFT de una institución financiera, a través del cual se identifiquen las áreas clave de posibles actividades de lavado de dinero y financiamiento del terrorismo. La base de un buen programa de cumplimiento ALD yace dentro de la evaluación del riesgo ALD.

Al evaluar el riesgo, es importante recordar algunas áreas dentro de la industria de servicios financieros que presentan un riesgo de posible lavado de dinero y financiamiento del terrorismo mayor que el de otras áreas, en razón de la naturaleza inherente de los tipos de negocios y transacciones involucradas. Estas áreas de mayor riesgo merecen un nivel de atención mayor y debe aplicarse un mayor escrutinio dentro del proceso de evaluación del riesgo. Las áreas dentro de las instituciones financieras que tienen un escaso o ningún riesgo ALD o CTF deben recibir la atención adecuada conforme a ellas.

Fundamentos de la evaluación del riesgo ALD

Partiendo de la base de que no hay un único proceso que se aplique a todas las instituciones y que ningún enfoque o metodología es absoluto, el fundamento de una evaluación efectiva del riesgo ALD debería incluir, como mínimo, los siguientes factores de riesgo:

- Tipos de clientes a los que se les prestan servicios bancarios
- Productos y servicios ofrecidos
- Alcance geográfico

Debería analizarse la base de clientes de la institución financiera. Como los clientes de alto riesgo conllevan un mayor riesgo de posible lavado de dinero y financiamiento del terrorismo, debería aplicarse un mayor escrutinio sobre las cuentas de los Negocios de Servicios Monetarios (NSMs), las Personas Expuestas Políticamente (PEPs), las Embajadas y Consulados Extranjeros (ECC) y las Compañías Privadas de Inversión (PICs, por sus siglas en inglés), por nombrar solo algunas. Estos tipos de clientes debería ser identificados, y su tipo de riesgo calificado conforme a su identificación. Además, todos los clientes de alto riesgo identificados como tales por la institución financiera, deberían ser analizados y también debería catalogarse su riesgo.

> Esto lleva a realizar un análisis cualitativo y cuantitativo de la revisión de la información

La cantidad de productos y servicios de alto riesgo ofrecidos por las instituciones financieras se correlata directamente con el riesgo ALD y CFT de la institución. Junto con los productos y servicios ofrecidos, también debería analizarse el procesamiento de las transacciones. La cantidad de transferencias, por ejemplo, debería ser identificada, analizada y evaluada dentro de la evaluación del riesgo. Estas transacciones incluyen las transferencias electrónicas locales e internacionales. Además, las Transacciones ACH y las Transacciones Internacionales ACH (IAT, por sus siglas en inglés) deberían recibir el mismo escrutinio que las transferencias electrónicas. Más aún, se recomienda analizar cuidadosamente cualquier iniciativa de productos nuevos o productos y servicios que recientemente se hayan convertido en "temas candentes" dentro de la industria, como la Captura Remota de Depósitos *(Remote Deposit Capture*, o RDC, por sus siglas en inglés), los Procesadores de Pagos de Terceros (*Third Party Payment Processors*, o TPPP, por sus siglas en inglés), los Embarques de Grandes Volúmenes de Dinero en Efectivo (Bulk Shipment of Currency, o BSC, por sus siglas en inglés) así como también las IAT mencionadas anterior-

mente. Es igualmente importante analizar los tipos de productos que se encuentran en estado de desarrollo y los productos emergentes, como los movimientos electrónicos de fondos y los pagos móviles, ya que estas clases de productos tienden a ser conductos o canales para los posibles lavadores o financistas del terrorismo debido a que los controles y las mitigaciones todavía pueden estar en fase de desarrollo.

La presencia de la institución financiera, su actividad en regiones conocidas por el tráfico de drogas y/o delitos financieros, así como también su exposición en el exterior, juegan un rol fundamental en la evaluación del riesgo ALD/CFT. También es importante e imperativo analizar la exposición de la institución financiera a los países de alto riesgo, los países en conflicto, y aquellos países o regiones en los cuales sus gobiernos hayan aplicados sanciones o boicot.

El tamaño y complejidad de una institución pueden ser un factor en la evaluación del riesgo ALD y CFT de la institución financiera. Las instituciones financieras más grandes y complejas, con presencia internacional, pueden querer evaluar su riesgo a nivel de sus unidades de negocios. Teniendo en cuenta que los reguladores están requiriendo una evaluación de riesgo ALD a nivel general de la empresa, la aplicación de la calificación del riesgo a nivel de la unidad de negocios sería una opción viable dentro de este enfoque. Las instituciones financieras más pequeñas y menos complejas pueden querer evaluar su riesgo solamente a nivel corporativo. Sin perjuicio del enfoque aplicado, la evaluación final del riesgo debe abarcar una evaluación general a nivel de la empresa del riesgo ALD y CTF. El elemento importante a recordar es que no existe un único enfoque que sea el correcto.

Se recomienda un enfoque basado en tres elementos para la elaboración de la evaluación del riesgo ALD de la institución financiera:

Fase 1 — Obtención de información y riesgo inherente

La primera fase para la elaboración de la evaluación del riesgo ALD es la obtención de información. Antes de evaluar el riesgo de la institución debe obtenerse un inventario completo de la base de datos de la institución financiera, los productos y servicios ofrecidos y las localidades geográficas. Debe establecerse un conocimiento cabal de la base de clientes, las clases de transacciones que utilizan y los volúmenes de las transacciones. También debe obtenerse y contarse con la información sobre la presencia geográfica de la institución financiera, la exposición en el extranjero y los bienes bajo su administración. Una vez trazado el mapa de la presencia y dónde desarrolla actividades la institución financiera, creada la lista de productos y servicios ofrecidos e identificados los clientes, recién entonces se cuenta con el conocimiento y las herramientas necesarias para evaluar efectivamente el riesgo inherente ALD y CFT de la institución financiera.

La metodología recomendada para conocer y analizar el riesgo inherente de una institución financiera puede dividirse en dos partes.

Primero, hacer una encuesta o entrevistar a aquellas unidades de negocios dentro de la institución financiera que hayan sido identificadas por serles aplicables el riesgo ALD o CTF. Hay que asegurarse de hacer participar a los gerentes de las unidades de negocios que corresponda, los oficiales de cumplimiento y los expertos en los temas específicos responsables de mitigar el riesgo ALD y CTF y el conocimiento para responder efectivamente y explicar el perfil de sus unidades de negocios. Estos individuos deben poder expresarse sobre la base de clientes, los productos y servicios ofrecidos, así también como la presencia geográfica y el alcance internacional de sus unidades de negocios.

Segundo, solicitar informes sobre los datos de los sistemas de administración de datos corporativos *(management information systems*, o MIS por sus siglas en inglés) para cuantificar los montos en dólares, los volúmenes de las transacciones y la cantidad de cuentas sobre cada factor de riesgo individual. Estos informes pueden servir como documentación respaldatoria de lo que se ha conocido mediante la entrevista o encuesta de la unidad de negocios. Esto lleva a realizar un análisis cualitativo y cuantitativo de la revisión de la información.

Al evaluar el riesgo y analizar las transacciones, hay que asegurarse de entender dónde se realizan las transacciones, quién tiene la propiedad para controlar y mitigar el riesgo. Esta transferencia o concepto de riesgo compartido incluye, pero no está limitada a, las oficinas de apoyo de las unidades de negocios y a las unidades de negocios que sirven como canales de entrega de los productos o las prestaciones de servicios. Es importante asignar y distribuir el riesgo de manera precisa y efectiva. En muchos casos, una unidad de negocios puede ser titular de la relación con el cliente. Sin embargo, a transacción o el servicio pueden ser ofrecidos o prestados dentro de otra unidad de negocios.

Las unidades de soporte de negocios a menudo tienen contacto con el cliente y en muchos casos realizan transacciones comerciales a pedido de y para el beneficio de un cliente. Las unidades de negocios que son titulares de la relación con el cliente no siempre son responsables o conocen a los productos o servicios que sus clientes están utilizando porque los mismos son brindados mediante otros canales. Como resultado de ello, el riesgo del producto o servicio debe ser asignado adecuadamente al canal de entrega correspondiente responsable de la

transacción o servicio. Esta metodología transfiere el riesgo de la unidad de negocio titular de la relación con el cliente a la unidad de negocios que efectivamente procesa la transacción en nombre de o en beneficio del cliente. En esos casos, la mitigación del riesgo pertenece a la unidad de negocios responsable del proceso.

Fase 2 — Mitigación del riesgo y evaluación del control

La segunda fase de la elaboración de la evaluación del riesgo ALD de la institución financiera es la explicación de los controles de mitigación del riesgo para defenderla contra las actividades ilegales. Estos controles incluyen políticas y procedimientos, monitoreo de transacciones y cuentas, unidades de investigación y programas de capacitación. Ahora es el momento de mencionar los controles que la institución financiera aplica para mitigar su riesgo de lavado de dinero y financiamiento del terrorismo. Los controles ALD y CTF son un factor importante para evaluar el riesgo de la institución financiera. Aunque muchas áreas de los servicios bancarios y financieros pueden ser inherentemente riesgos cuando se habla de lavado de dinero y financiamiento del terrorismo, los controles para mitigar el riesgo, aplicados adecuadamente pueden ayudar a neutralizar ese riesgo, disminuyendo así el nivel de riesgo dentro de esa área de servicio.

Un programa ALD efectivo debería incluir las siguientes estrategias de respuesta al riesgo o componentes de riesgo:

- Programa de Identificación del Cliente (PIC)
- Debida Diligencia sobre el Cliente (DDC)
- Debida Diligencia Reforzada (DDR)
- Política ALD y Dirección del Programa
- Monitoreo e Investigación de Transacciones (UIF)
- Leyes y Boicots y Sanciones a Países o Regiones (OFAC)
- Reporte Regulatorio (ROS) (RAS)
- Conservación de Registros y Registración

Además de las responsabilidades de cumplimiento mencionadas anteriormente, el riesgo del producto, servicio y cliente también debe ser monitoreado y también debe calificarse ese riesgo. Un enfoque y metodología recomendada es graficar estos factores de riesgo y consolidarlos en componentes de riesgo o estrategias de respuestas al riesgo (ver figura 1). Esto permite una evaluación de estos factores de riesgo a nivel del componente y facilita el conocimiento del análisis del riesgo. Como los procesos y procedimientos generalmente son constantes para cada tipo de cliente, producto o servicio, sería redundante mostrar el PIC, la DDC y la DDR de cada uno de los clientes a los cuales se les prestan servicios bancarios. Es mejor consolidar todos los tipos de clientes en un solo grupo y calificar su riesgo de manera acorde.

Figura 1

Determinación del Factor de Riesgo con el Componente de Riesgo

La utilización de la metodología de determinación del factor de riesgo permite la posibilidad de evaluar tanto el riesgo inherente como el riesgo residual a nivel de componente. La inclusión de las clases de productos, servicios y clientes dentro del componente adecuado permite una calificación del riesgo inherente de acuerdo con varios factores de riesgo. Una vez que el riesgo inherente ha sido identificado por cada componente, la revisión de las políticas, procedimientos y con troles ayudará a asignar la calificación del riesgo residual de cada componente. Dependiendo de la efectividad de estos controles, se asignarán puntos de reducción del riesgo. Los controles pueden ser efectivos marginalmente efectivos o no efectivos, lo que muestra la cantidad de puntos de reducción del riesgo asignados, si hubiere. Como resultado de ello, la calificación del riesgo inherente menos los puntos de reducción del riesgo asignado equivale a una calificación del riesgo residual final.

Fase 3 — Diferencia en el análisis y planes de acción

La tercera y última fase en la elaboración de la evaluación del riesgo ALD de la institución financiera es la identificación de las áreas de exposición y las posibles brechas en las que el lavado de dinero o el financiamiento del terrorismo puedan encontrar los espacios a través de las cuales filtrarse. Este análisis de esos espacios que pudieren existir es conocer las áreas que necesitan un mayor escrutinio y controles más estrictos. Es importante recordar que la evaluación del riesgo ALD debería generar el programa de cumplimiento ALD. Es en la segunda fase de su evaluación de riesgo ALD que se comienza a lograr que la evaluación sea procesable. Al hacer eso, se empiezan a modificar o elaborar políticas, procedimientos, procesos y controles sobre aquellas áreas identificadas por tener un potencial riesgo de lavado de dinero y financiamiento del terrorismo. El nivel de riesgo identificado dentro de estos vacíos determina el nivel de diligencia debida requerida. Si el riesgo lo requiriera, debería aplicarse un plan de acción para mitigar el riesgo y cubrir esa brecha.

Calificación y puntaje del riesgo

Al establecer un criterio de calificación del riesgo o una metodología de puntaje del riesgo, el punto inicial de la matriz de calificación debería comenzar con los puntajes de calificación del riesgo de menor a mayor. La asignación de números para cada viable de calificación del riesgo ayuda a simplificar la suma del puntaje total de la calificación del riesgo de la empresa. Al asignar los números y la importancia a las variables de calificación del riesgo, a veces es mejor aplicar una simple ecuación

Ejemplo de Escala de Calificación de Cinco Puntos (figura 2)

- Puede ser Alfa (Menor a Mayor), (Mínimo a Extremo) o Numérica (1 – 5)
- También se recomienda la codificación por color
- Es importante incluir No Aplicable (NA) ya que esto demuestra que el riesgo no fue pasado por alto y fue calificado

Figura 2

Calificación del Riesgo		
Bajp	B	1
Bajo / Moderado	B/M	2
Moderado	M	3
Moderado / Alto	M/A	4
Alt	A	5
No Aplicable		

Reuniendo todos los elementos

Si la evaluación del riesgo se realizara a nivel de la unidad de negocios, debería asignarse a cada unidad de negocios los componentes

aplicables y el riesgo evaluado correspondiente. Como alternativa, puede utilizarse este mismo enfoque a nivel del segmento del negocio o a nivel corporativo, según el tamaño y complejidad de la institución financiera. Sin embargo, si una institución financiera requiriera una evaluación a nivel de la unidad de negocios o del segmento del negocio, se recomienda crear un perfil a nivel de la empresa de todas las unidades de negocios evaluadas con una calificación del riesgo corporativo general. Un perfil consolidado de todas las unidades de negocios evaluadas permite dirigir a la compañía con una visión de la de la empresa sobre dónde existe el riesgo. Además, esa visión apunta a las unidades de negocios con múltiples factores de riesgo en relación con otras unidades de negocios. Esto puede requerir una atención adicional para aquellas unidades de negocios.

El programa de cumplimiento ALD y la evaluación del riesgo ALD deberían funcionar juntos. Ésta es la oportunidad de evaluar el riesgo ALD y CFT de la institución financiera y reforzar los controles en los casos que sea necesario. La evaluación de estos riesgos se convierte en el fundamento para establecer un programa de cumplimiento ALD exitoso. La evaluación del riesgo ALD de la institución financiera debería servir como paraguas del programa de cumplimiento ALD. Además, también puede ser utilizado como un manual de referencia que identifique rápidamente la exposición al riesgo de la institución financiera, así también como servir como una referencia rápida sobre dónde se ofrecen los productos y servicios, qué unidades de negocios están prestando servicios bancarios a los clientes de alto riesgo, y cómo son las presencias geográficas, entre otra información importante que compone el perfil corporativo.

Mediante la evaluación del riesgo ALD, se ofrece una explicación de cualquier riesgo ALD o CFT presentes y los controles aplicados para mitigar esos riesgos. Un comentario bien elaborado y una explicación que la respalde para atender los riesgos y los controles alrededor de esos riesgos ayuda a los examinadores regulatorios a conocer el negocio, la compañía y su iniciativa del programa de cumplimiento ALD. Además, este mismo enfoque ofrece un resumen ejecutivo de alto nivel para la gerencia ejecutiva interna, así también como para el Oficial Jefe LSB o el Director ALD. Más aún, hay que hacer referencia a los materiales utilizados en la etapa de obtención de información. Documente lo que ha encontrado y adjunte o mencione los materiales de referencia. Una explicación clara del riesgo, respaldado con los documentos con las conclusiones, hace que los lectores tengan un documento de fácil comprensión.

La evaluación del riesgo ALD debería tener una conclusión. La evaluación también debería identificar el nivel de riesgo ALD y CTF presentes dentro de la institución financiera así como también asignar un puntaje final a la calificación del riesgo. El puntaje final de la calificación del riesgo debería identificar a las calificaciones del riesgo inherentes y residuales de la institución financiera y las vulnerabilidades ante la posibilidad de ser utilizada para lavar dinero proveniente de actividades ilegales o de realizar financiamiento del terrorismo. Además, hay que incluir una explicación del criterio para la calificación. Hay que explicar si se han asignado valores numéricos para identificar los niveles de riesgo o si un factor ha sido tenido más en cuenta que otros.

> La evaluación del riesgo ALD ayudará a aplicar el programa de cumplimiento ALD

Una vez que la evaluación del riesgo ALD ha sido completada, hay que llevarla a la práctica y aplicarla. La Evaluación del Riesgo ALD debería ser un documento suficiente. Como mínimo, la evaluación del riesgo ALD y CTF debería realizarse cada 18 meses o anualmente en el caso de las instituciones financieras más grandes. Los riesgos deben ser reevaluados a medida que cambia el negocio. Los cambios dentro de la institución financiera deben ser acompañados de un cambio proporcional en la Evaluación del Riesgo ALD. Como resultado del ritmo cambiante en la industria financiera, la evaluación del riesgo ALD tiene una expectativa de vida limitada. Debería ser revisada de acuerdo con las circunstancias y mantener el ritmo de los cambios y complejidades del riesgo ALD y CTF.

Conclusión y comunicaciones

Los resultados de la evaluación del riesgo ALD ayudarán en la evolución del programa de cumplimiento ALD. Brindarán información para la planificación y las prioridades dentro de las áreas, como:

- Mejoras en los procedimientos de las unidades de negocios
- Planificación de los controles y alcance y cobertura del examen
- Oportunidades de capacitación
- Monitoreo adicional o reforzado de las transacciones

Dentro de la conclusión y las opiniones de la empresa, un mapa de riesgo debería servir como brújula, permitiéndole a la gerencia ejecutiva ver en qué dirección debería estar mirando. El riesgo asignado en forma precisa a aquellas unidades de negocios que tienen clientes, canales de entrega correctamente identificados y áreas de soporte responsables de productos, servicios, clientes o procesos a los cuales brindan apoyo claramente descriptas permiten un análisis del riesgo efectivo y preciso. Además, es fundamental volver a explicar las conclusiones en un resumen descriptivo ejecutivo de alto nivel, concentrándose en aquellas áreas que necesitan más atención. Como resultado de ello, la gerencia puede dirigir más efectiva y eficientemente el riesgo ALD y CFT presentes dentro de la institución financiera.

Por último, es fundamental comunicar los resultados de la evaluación del riesgo ALD a la gerencia y a las unidades de negocios involucradas e identificadas con riesgo ALD y CFT aplicables. Esta comunicación debe ser realizada con un enfoque desde las instancias jerárquicas superiores hacia los estratos inferiores.

Anthony J. Tricaso, CAMS, analista senior LSB/ALD y OFAC, Key BankCleveland, Ohio EE.UU., Anthony_j_tricaso@keybank.com

Desmistificando a la transferencia electrónica para los investigadores

Las investigaciones de lavado de dinero sin duda implicarán una revisión en algún momento de las transferencias electrónicas (denominadas a veces "transferencias electrónicas de fondos"). Las transferencias electrónicas han sido un medio común de lavado de dinero hacia cuentas offshore en jurisdicciones conocidas por ser paraísos de secretismo bancario.

Una transferencia electrónica es iniciada con una solicitud de un cliente de dirigir la transferencia de fondos a otro lugar, sea local o internacional. La solicitud, usualmente realizada a través de un banco o una institución financiera similar, indica instrucciones a través de un sistema de mensajes por teléfono, correo electrónico, fax u otro medio electrónico de comunicación. Antes de que los fondos lleguen a su destino final, los fondos pueden trasladarse a través de varias instituciones financieras y jurisdicciones de tránsito, utilizando cuentas bancarias corresponsales, transferencias seriales, pagos de cobertura, compañías pantalla y jurisdicciones offshore. Esta característica ha hecho que las transferencias electrónicas, al menos en el pasado, fueran atractivas para los lavadores de dinero, agregándole complejidad en el ocultamiento, la segunda fase del ciclo de lavado de dinero. En algunos casos, algunas instituciones financieras inescrupulosas han facilitado la transferencia de fondos obtenidos ilegalmente ayudando a los criminales a lavar los fondos a través de complejas transacciones, utilizando vehículos corporativos y estableciendo privilegios especiales en cuentas de bienes privados.

Si bien ha habido esfuerzos en los últimos años para codificar la información en el mensaje de la transferencia electrónica que pueda permitirle a los investigadores rastrear mejor la fuente y destino de los fondos, es de gran ayuda para el investigador conocer más cabalmente cómo operan las transferencias cablegráficas y qué información está disponible realmente.

Una transferencia electrónica tiene dos componentes: (1) la instrucción, que incluye información sobre tanto la institución originadora como la beneficiaria, y (2) el movimiento real o transferencia de fondos. Las instrucciones pueden ser enviadas de varias maneras, generalmente a través de una institución financiera, a través de redes electrónicas de comunicación, correo electrónico, fax, teléfono, telex u otros varios sistemas interbancarios de pagos. El método más utilizado en la industria bancaria para comunicar las instrucciones de transferencia es a través del uso de un sistema especial de telecomunicaciones financieras conocido como la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales *(Society for Worldwide Interbank Financial Telecommunications*, o SWIFT", por sus siglas en inglés). Debe señalarse que SWIFT opera solo como un servicio de mensajería — no tiene ni administra cuentas y no participa en sí mismo en la transferencia efectiva de fondos. La transferencia efectiva se realiza a través del uso de relaciones de corresponsalía, lo que será analizado a continuación.

SWIFT puede ser utilizado para las transferencias domésticas y las internacionales; sin embargo, algunas jurisdicciones tienen disponibles sistemas de pagos interbancarios alternativos. Por ejemplo, en los Estados Unidos, existe al menos otros dos sistemas de pagos bancarios a disposición: la Casa de Compensación del Sistema de Pagos Interbancarios *(Clearing House Interbank Payments System*, o CHIPS, por sus siglas en inglés y el Servicio de Fondos *(Fedwire Funds Service*, o Fedwire). La principal diferencia entre estos dos sistemas y el de SWIFT es que tanto el CHIPS como el Fedwire pueden participar más en la transferencia efectiva de los fondos. Además, el sistema de pago directo de banco-a-banco y otros sistemas de pago intermediarios son utilizados por los bancos para transferir los fondos entre las instituciones.

La transferencia efectiva de los fondos se realiza a través de lo que se denomina "transferencia de libro". Una transferencia de libro es básicamente un proceso contable que físicamente mueve los fondos de una cuenta a otra. Si tanto el cliente originador como el cliente beneficiario tienen una cuenta en la misma institución financiera, entonces una transferencia de libros interna puede realizarse entre las dos cuentas del cliente. Cuando los fondos son transferidos entre dos instituciones financieras no relacionadas, la transferencia de libro se realiza través de un banco corresponsal o intermediario empleado para vincular la relación.

En los Estados Unidos, muchos bancos tienen cuentas corresponsales con el propósito de procesar y compensar transacciones de transferencias electrónicas con otras instituciones que son miembros de y tienen acceso a CHIPS o Fedwire. Esto les permite realizar transferencias electrónicas en nombre de sus clientes, aún cuando ellas mismas no sean instituciones miembros. Las relaciones de banca corresponsal se dan por lo general entre bancos locales y bancos extranjeros porque pueden facilitar los negocios y brindar servicios a los calientes en jurisdicciones extranjeras sin los gastos ni la carga de que un banco tenga que establecer una presencia en el extranjero. Estas relaciones de banca corresponsal pueden luego consumar la transferencia de fondos que ha sido autorizada a través de SWIFT u otros sistemas. Si los dos bancos no tienen una relación directa de banca corresponsal entre ellos, entonces pueden darse relaciones con otros bancos que sí tengas esas relaciones de banca corresponsal y pueden utilizar a esos otros bancos como terceros para efectuar la transferencia efectiva de los fondos.

Decodificando la instrucción de la transferencia electrónica

Muchas instituciones financieras han tratado de incorporar dispositivos antilavado de dinero en sus procedimientos de transferencias electrónicas. Actualmente, en muchas jurisdicciones, los bancos y otras instituciones financieras están obligados a obtener cierta información sobre el cliente y el monto, fuente y propósito de los fondos transferidos, así también como información sobre el beneficiario. Esta información generalmente es requerida para ser conservada y disponible en caso de surgir alguna investigación. Además, el banco o la institución financiera conservarán su propia documentación, como los resúmenes de aviso confirmando las transferencias electrónicas y los memos de débitos y créditos enviados por los bancos a sus clientes originadores o beneficiarios. Estos documentos pueden ser útiles para determinar los números de cuentas y la identidad de los clientes originadores y beneficiarios. Cuando esos documentos no están disponibles, el proceso de identificación y rastreo de los fondos necesitará un conocimiento de cómo leer e interpretar los distintos sistemas de mensajes utilizados para realizar las transferencias electrónicas.

Los sistemas de pago como el CHIPS y Fedwire utilizan un formato de mensaje distinto para las comunicaciones de transferencias electrónicas entre las instituciones miembro. SWIFT ha implementado una plataforma de mensajería estandarizada utilizada por las instituciones financieras en todo el mundo. Dentro de los mensajes de SWIFT, existen protocolos generales de la industria para los formatos de los mensajes, códigos especiales para diferencia entre la información y la dirección, y encriptado para prevenir las fallas de seguridad durante la transmisión de los datos. Para identificar los distintos tipos de mensajes SWIFT, existen números asignados a cada uno de ellos. Por ejemplo, si un mensaje es identificado como "MT 103", el prefijo "MT" indica "tipo de mensaje" y el número de tres dígitos que sigue denota una clase específica de mensaje SWIFT (en este caso, "103" significa una única transferencia de cliente/crédito). Dentro del tipo de mensaje, se utilizan campos específicos de códigos para demarcar información importante. El campo 50 es un campo importante sobre el cual hay que concentrarse porque incluye información sobre el nombre y domicilio del cliente que ordena la operación. Dado que es un campo abierto, a menudo puede incluir información sobre la identificación del cliente requerida por la ley o por las políticas internas de una institución. Esto puede ser de utilidad para identificar a la persona en particular que autoriza la transferencia, en el caso de una entidad corporativa o como identificadores útiles para distinguir a un cliente de aquellos otros clientes que tengan nombre similares.

Los códigos identificadores de bancos de SWIFT (BICs, por sus siglas en inglés) son otra fuente para los profesionales porque contienen el nombre de la institución financiera, la jurisdicción, localidad y/o sucursal. Los BICs generalmente tienen una extensión de ocho caracteres y consisten en un código bancario (único para la institución financiera), un código de país (para identificar la jurisdicción donde se encuentra la institución financiera), y un código de lugar (que indica una distinción geográfica dentro de una jurisdicción). A veces, se utilizan tres

caracteres adicionales para un código de sucursal (para identificar la sucursal física de una institución financiera).

El cuadro a la derecha muestra un ejemplo de cómo es un mensaje SWIFT y algunos códigos comunes utilizados allí:

:20:	PAYREF XT78305
:32A:	091010EUR#1010000#
:50:	[Nombre y domicilio del cliente]
:59:	[Nombre y domicilio del beneficiario]

Interpretación de Código

20	Número de referencia de transacción (número codificado asignado por la institución originadora para identificar la transacción)
32	Fecha del valor, código de moneda y monto de la transacción
50	Cliente que ordena la transacción (parte que ordena la transacción SWIFT)
59	Beneficiario (parte designada como el último receptor de los fondos)

Además de los códigos anteriores, otros códigos pueden incluir

52D	Banco originador (institución financiera que inicia el SWIFT)
53D	Banco corresponsal del remitente
54D	Banco corresponsal del receptor
57D	La institución financiera en donde el cliente que orden la transacción solicita que se pague al beneficiario
70	Detalles del pago
71A	Detalles de los cargos de la transacción
72	Instrucciones del banco remitente al banco receptor

Investigación adicional

en muchos casos, el investigador necesitará acceder a los registros bancarios más allá del mensaje mismo de transferencia.

Los registros importantes pueden encontrarse tanto en la institución originadora como en la institución beneficiaria o receptora. Si algún banco intermediario o corresponsal fuere utilizado en la transferencia, también deberían obtenerse sus registros. En el caso de los documentos de la institución originadora, tenga presente analizar lo siguiente:

- Formulario de solicitud de transferencia de fondos
- Copia de la transferencia electrónica
- Resumen de aviso o confirmación de la transferencia electrónica
- Memo de débito al cliente originador
- Resumen mensual de cuenta del cliente
- Registro interno de las transferencias salientes (registros de bancos corresponsales, registros de pagos y procesamientos)
- Registro en el libro diario

Para los documentos de la institución beneficiaria o corresponsal, el investigador puede querer revisar:

- Formulario de solicitud de transferencia de fondos
- Copia de transferencia electrónica
- Memo de crédito al cliente beneficiario (si fuere depositado)
- Resúmenes mensuales de la cuenta del cliente
- Registro en el libro diario
- Cheques de cajero
- Información de la transferencia de libro interbancaria que conservan los bancos con el fin de realizar las transacciones de compensación

Además, dependiendo de las circunstancias de la investigación, puede ser importante obtener documentos suplementarios adicionales que pudieren estar disponibles, como ser:

- *Documentos de pagos subyacentes.* Facturas, documentos de embarque, recibos contratos de consultoría y otros documentos asociados con una transferencia pueden revelar información importante sobre los fondos en cuestión.
- *Información sobre el Conozca a Su Cliente o "CSC".* A nivel de la transacción, el banco puede no haber identificado al beneficiario final cuando los fondos salieron de la cuenta. La información CSC también puede ser útil con relación a esto.
- *Transferencias de libro entre las cuentas personales y corporativas.* Esas transferencias pueden ser útiles para detectar un esquema de ocultamiento.
- *Entradas privadas y variantes de nombres en SWIFT utilizadas por la institución financiera.* Una revisión de las distintas entradas de SWIFT utilizadas solamente para los clientes de banca privada dentro del banco y sus diversas sucursales puede descubrir un potencial permiso especial distinto para la transacción originada a través de estas entradas. Las variantes de nombres SWIFT utilizadas por la institución financiera pueden reveler las transferencias a través de distintos canales. Un banco puede tener diferentes departamentos de transferencias electrónicas, domicilios o formas internas de identificarse. Para asegurar que las entradas y las variantes de nombres estén listadas a fin de generar registros bancarios, los profesionales deberían considerar obtener esta información a través de entrevistas con funcionarios del banco.
- *Reportes de operaciones sospechosas (ROSs).* Cuando estuvieren disponibles, los ROSs o los informes de inteligencia pueden revelar información valiosa sobre las transferencias electrónicas y detalles de quien origina la operación.
- *Patrones de transacciones en determinadas instituciones.* Cuando se analice la información obtenida de los bancos más pequeños, los profesionales pueden buscar patrones de transferencias por montos importantes en relación con el tamaño del banco (por ejemplo, una transferencia de libro que sea el 80% del dinero total transferido a un banco determinado durante un mes).
- *Transferencias corregidas, devueltas o reenviadas.* Los sistemas de monitoreo creará advertencias o avisos de alerta para los mensajes que contengan errores (como la información incompleta del originador). Esos mensajes son luego separados y alertados para proceder con su revisión manual. Dichos documentos a menudo son mantenidos por los bancos originadores y beneficiarios y pueden revelar patrones de actividad por parte del investigado o del banco.

Kenneth Barden, JD, CSAR, CAMS, Modernizing Financial Institutions Project, Washington, DC, EE.UU., kennethbarden@gmail.com

Inversiones extranjeras directas y tendencias de lavado de dinero

Este artículo analiza la relación entre las Inversiones Directas Extranjeras (FDIs) y el lavado de dinero a escala global. Ha habido un debate sobre si los centros de lavado de dinero atraen a las inversiones extranjeras con el objeto de ocultar los orígenes ilícitos de los fondos o si existe una tendencia global menores inversiones extranjeras hacia jurisdicciones de lavado de dinero con controles laxos de lavado de dinero por los riesgos reputaciones que presentan los centros de lavado de dinero. El análisis de este tema se basará en el documento sobre las FDIs titulado *Lavado de Dinero como Móviles para las FDIs (Money Laundering as Motives for FDIs)* y sobre un análisis de casi 60.000 proyectos de FDI s que se realizaron globalmente entre 2003 y 2008.

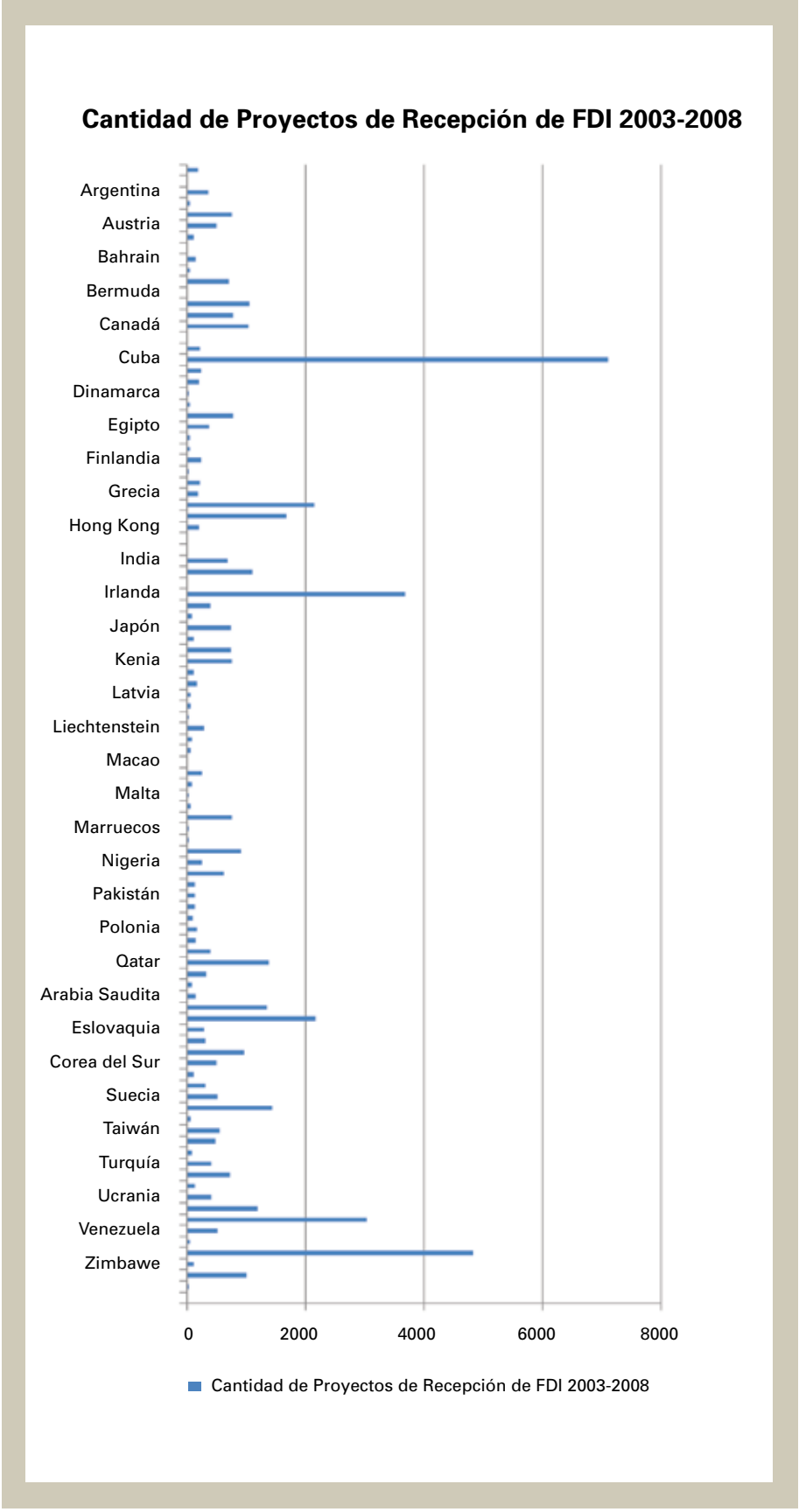
Flujos de dinero ilícito como móviles para las FDIs

Existen unos pocos estudios empíricos entre la bibliografía sobre la FDI que se concentren sobre los flujos de dinero ilícito como un determinante para las FDIs. Uno de los documentos de trabajo más destacados sobre este tema en términos de sus conclusiones es *Flujos de Dinero Ilícito como Móviles para la FDI (Illicit Money Flows as Motives for FDI)* de Joseph C. Brada (Universidad del Estado de Arizona), Zdenek Drabek (Organización Mundial del Comercio y M. Fabio Pérez (Universidad Wilfrid Laurier), donde se analiza el rol de la FDI en la facilitación del lavado de dinero y la salida de capital utilizando los flujos salientes de FDI en las economías de transición muestran en qué medida la FDI es generada por estos móviles. Sus conclusiones son muy interesantes, ya que sugieren que los flujos de dinero ilícito influyen tanto en la elección de los países receptores de la FDI como en el volumen de los flujos de FDI hacia esos países. Su trabajo estima que el 10 por ciento del total de flujos de FDI y más de la mitad de la FDI hacia países de lavado de dinero tienen como objetivo facilitar los flujos de dinero ilícito.

Etapas de lavado de dinero, compañías pantalla, fideicomisos nominados y otros vehículos corporativos

Las inversiones extranjeras por su naturaleza pueden ser utilizadas con fines de lavado de dinero en varias etapas del ciclo de lavado de dinero. Comparadas con otros métodos de lavado comúnmente conocidos, la cantidad de dinero involucrados en inversiones extranjeras es sustancialmente alta ya que estos fondos son utilizados para adquirir fábricas, edificios de oficinas, maquinarias, materiales de construcción y demás, dependiendo de la industria, dándole a la inversión un aire de legitimidad. Esto puede lograrse a través de la creación de compañías pantalla en la etapa de colocación que puedan mezclar estos fondos con sus ganancias (si las hubiere) o utilizar solamente los fondos ilícitos para invertir en jurisdicciones transfronterizas con el propósito de ocultar su verdadero origen. Para ocultar a los propietarios, podrían utilizarse fideicomisos, nominados y otros vehículos corporativos, los cuales se encuentran entre los métodos más comúnmente conocidos asociados con el lavado de dinero. Estas inversiones pueden ser utilizadas definitivamente en la etapa de integración del lavado de dinero, así como través a través de las ventas de estas inver-

Cuadro 1 — Cantidad total de proyectos de recepción de FDI por país.



siones, sea que se trate de asociaciones comerciales o adquisiciones de negocios en los países receptores. La evasión fiscal es otro facilitador importante de las decisiones en la FDI y las transferencias de fondos hacia jurisdicciones con controles y regulaciones deficientes sobre el lavado de dinero.

Utilización de la banca corresponsal

A fin de facilitar la transferencia de estos fondos hacia países receptores o centros de lavado de dinero, es común la utilización de la banca corresponsal, ya que es poco probable que los negocios de servicios monetarios sean utilizados para transferir esas sumas elevadas de dinero ya que atraerían más sospechas sobre los mismos. En lugar de ello, un banco importante y reconocido que tenga una relación de corresponsalía bancaria con un banco corresponsal local de la jurisdicción destinataria es más probable que sea elección del lavador de dinero.

Las FDIs y el riesgo reputacional del país receptor

El otro lado del debate sugiere que dados los riesgos reputacionales que presentan las jurisdicciones con controles y regulaciones deficientes sobre el lavado de dinero, habrá consecuencias sociales y económicas incluidas el debilitamiento del crecimiento y desarrollo económico en estos países. La mayoría de las instituciones financieras probablemente restrinjan las transacciones con negocios en estos países a fin de mitigar su propio riesgo, así también como para cumplir con las regulaciones locales e internacionales sobre ALD y contra el financiamiento del terrorismo (CTF). En este caso, los lavadores podrían ni siquiera tener acceso a invertir en estas jurisdicciones por las prohibiciones y restricciones. Además, los países que tengan mala reputación o publicidad adversa contra ellos probablemente se vuelvan riesgosos para invertir en negocios en ellos.

Patrones globales de inversión extranjera directa

A fin de investigar qué lado del debate está más cerca de la realidad, es fundamental analizar los proyectos globales de inversiones extranjeras directas que están integrados por la fuente y países de destino, los proyectos globales de FDI así como también las sumas totales invertidas a través de las fronteras.

Cuadro 2 — Cantidad total de proyectos de recepción de FDI entre 2003 y 2008

Nombre del País	Cantidad de proyectos de recepción de FDI 2003 – 2008	Nombre del País	Cantidad de proyectos de recepción de FDI 2003 – 2008	Nombre del País	Cantidad de proyectos de recepción de FDI 2003 – 2008
Argelia	182	Guyana	9	Pakistán	168
Antigua	0	Hong Kong	685	Perú	157
Argentina	355	Hungría	1113	Filipinas	396
Armenia	51	Islandia	14	Polonia	1385
Australia	757	India	3679	Portugal	319
Austria	496	Indonesia	393	Puerto Rico	83
Azerbaiján	116	Irán	85	Qatar	156
Bahamas	7	Irlanda	732	Rumania	1346
Bahrain	156	Israel	115	Rusia	2166
Bangladesh	49	Italia	735	Arabia Saudita	287
Bélgica	701	Japón	761	Serbia & Montenegro	305
Bermuda	6	Jordania	108	Singapur	975
Brasil	1046	Kazakhstán	162	Eslovaquia	505
Bulgaria	778	Kenia	67	Eslovenia	109
Canadá	1042	Kuwait	70	Sudáfrica	311
Islas Caimán	3	Kyrgyzstán	19	Corea del Sur	523
Chile	226	Latvia	294	España	1428
China	7102	Líbano	80	Sri Lanka	59
Colombia	243	Libia	70	Suecia	551
Croacia	196	Liechtenstein	2	Suiza	478
Cuba	19	Lituania	246	Siria	77
Chipre	41	Luxemburgo	71	Taiwán	415
República Checa	781	Macao	31	Tailandia	719
Dinamarca	384	Macedonia	67	Túnez	126
República Dominicana	47	Malasia	755	Turquía	416
Ecuador	43	Malta	36	Emiratos Árabes Unidos	1192
Egipto	237	Mauricio	26	Reino Unido	3040
El Salvador	29	México	922	Ucrania	522
Estonia	226	Marruecos	260	Uruguay	45
Finlandia	179	Holanda	611	EE.UU.	4828
Francia	2144	Nueva Zelanda	135	Venezuela	117
Alemania	1681	Nigeria	127	Vietnam	995
Grecia	197	Noruega	128	Yemen	22
Groenlandia	5	Omán	99	Zimbawe	13

Datos y análisis

La información fue obtenida de OCO Monitor, fDi Markets, que es la base de datos más completa que contiene datos sobre la compañía fuente, el país fuente, país de destino, cantidad de proyectos FDI, así también como los puestos de empleo creados. En total, entre 2003 y 2008, se registraron globalmente casi 60.000 proyectos de FDI. La información también fue utilizada en el documento de trabajo: *Efectos de las Inversiones Directas Extranjeras de Compañías Multinacionales por Desempeño de Compañía y por Crecimiento Económico del País (Effects of Foreign Direct Investments by Multinational Companies on Company Performance and on country Economic Growth)* de Ayse Yuce (Escuela de Administración Ted Rogers) y Vefa Buyukalpelli (UIF Global ALD, Royal Bank of Canada).

Cuadro 1. TOTAL FDI (2003 – 2008)	
Cantidad total de compañías incluidas en la base de datos	19,961
Cantidad total de proyectos FDI (2003 – 2008)	58,204

El análisis incluye un total de 58.204 proyectos de inversión extranjera realizados por 19.961 compañías de 103 países entre 2003 y 2008. El Cuadro 2 y la Figura 1 ilustran la cantidad total de proyectos de recepción de FDI entre 2003 y 2008.

Al interpretar estas estadísticas, es fundamental recordar que existen varios factores involucrados en las decisiones de inversión, y el propósito aquí es demostrar los patrones de inversión en las jurisdicciones calificadas como de alto riesgo en términos de lavado de dinero así también como en aquellas que tienen una calificación de riesgo menor. Un análisis detallado del Cuadro 2 muestra la baja cantidad de proyectos FDI en países de mayor riesgo que tienen regulaciones y controles laxos de lavado de dinero. Por ejemplo, Antigua no recibió ninguna inversión extranjera entre 2003 y 2008. Bahamas recibió 7, las Islas Caimán recibieron 3, Cuba 19, República Dominicana 47, Ecuador 43, El Salvador 29, Guyana 9, Irán 85, Kenia 67, Krgyzstán 19, Liechteinstein 2, Zimbawe 13, Yemen 22, Uruguay 45, Siria 77 y Sri Lanka 59. Nótese que estas cifras son muy bajas comparadas con los proyectos de recepción de FDI en países de menor riesgo que tienen una mayor estabilidad política y mejor reputación internacional.

Conclusiones e implicancias políticas

el análisis general de las tendencias de FDI y los estudios en bibliografía sobre las relaciones entre las inversiones extranjeras y el lavado de dinero revela que la inversión a través de las fronteras en las economías de transición ha sido utilizada con el propósito de ocultar las fuentes de los fondos ilegales y facilitar el ingreso de estos fondos en el sistema financiero pero no necesariamente hacia jurisdicciones reconocidas como centros de lavado de dinero.

Los gobiernos, los reguladores y las regulaciones internacionales (por ejemplo, las tipologías del GAFI, el Grupo Wolfsberg, el Comité de Basilea, etc.) tienen contramedidas para detectar y detener los métodos más conocidos de lavado de dinero. En el caso de la detección y la disuasión del lavado de dinero a través de las inversiones extranjeras, se requerirá un escrutinio más reforzado de estas entidades para poder lograr este objetivo. Una de las obligaciones más importantes de la diligencia debida sería auditar los estados financieros de las compañías cuya elección de lugar no tiene un sentido económico.

Los mayores determinantes de las FDIs como el costo laboral, la estabilidad política del país receptor, el costo de las materias primas, la rentabilidad, la decisión de los competi-

> En el caso de la detección y la disuasión del lavado de dinero a través de las inversiones extranjeras, se requerirá un escrutinio más reforzado de estas entidades para poder lograr este objetivo

> Si la inversión es en la forma de adquisiciones de entidades extranjeras, también debería auditarse la documentación asociada a ellas

dores, etc. son ampliamente conocidos y son factores de sentido común. Cualquier decisión de inversión que sea inusual en naturaleza o que tenga móviles irracionales puede indicar la existencia de lavado de dinero. Por lo tanto, las compañías de las economías de transición que invierten en otros países deberían estar sujetas a un escrutinio reforzado especialmente si las decisiones de inversión no tienen sentido económico o si hay evidencias de que el objetivo de esas inversiones no es generar ganancias.

Entre ellos, son fundamentales la auditoria de los balances, los estados de ingresos, los estados de ganancias obtenidos y los resúmenes de flujos de efectivo en línea con los Estándares Internacionales de Contabilidad. La verificación de la documentación y la facturación asociada con las adquisiciones de activos fijos, gastos prepagados, bienes raíces, seguros, pagos de salarios y servicios serán necesarias para confirmar que la compañía está invirtiendo con el propósito de generar ganancias. Si la inversión es en la forma de adquisiciones de entidades extranjeras, también debería auditarse la documentación asociada a ellas. Finalmente, otra contramedida para aquellas compañías que invierten en jurisdicciones de alto riesgo incluye el escrutinio reforzado de la estructura de propiedad, los accionistas y la junta directiva para mitigar los riesgos asociados con estas personas que son los controladores finales de la compañía, y quienes pueden posiblemente ser personas expuestas políticamente.

Vefa Buyukalpelli, CAMS, MA (Finance), Investigaciones ALD, UIF ALD Global, Royal Bank of Canada, Toronto, ON, Canadá, vefa.buyukalpelli@rbc.com

Legado de Napoleón:

Cómo el pensamiento del desvía el ALD en el siglo XXI

Nota del Editor: Este artículo es el primero de una serie que analiza cómo pueden los bancos evaluar mejor el riesgo geográfico. Tanto en el momento de incorporación del cliente como en el monitoreo de las transacciones, la geografía juega un papel clave en ayudar a que los bancos apliquen su enfoque basado en el riesgo en el cumplimiento ALD. El primer artículo analiza cómo determinan los bancos a qué países calificar por su riesgo.

En 1815, después de casi un cuarto de siglo de guerra constante, Napoleón estaba próximo a ser derrotado y Europa estaba arruinada. Austria, Francia, Rusia y el Reino Unido, las potencias más importantes de esa época, se reunieron en la capital austríaca para reunificar un continente fracturado. El Congreso de Viena volvió a trazar el mapa de Europa — colocando ducados y principados entre los países hasta que logró un débil equilibrio entre los intereses en pugna. Al final, emergió un sistema político que incluyó a 39 estados soberanos, y muchos más nobles que buscaban mejorar sus territorios para que pasaran a ser miembro pleno de este nuevo club internacional.

A primera vista, una reunión del siglo XIX de los actores poderosos europeos parecería que no tiene nada que ver con la lucha contra el lavado de dinero del siglo XXI. Pero cómo conceptualizan los bancos un riesgo geográfico, a menudo es un concepto que se conservó del pensamiento de esta época pasada.

¿Qué hace que un país sea un país?

Todos están de acuerdo en que Francia es un país. Benín también lo es. ¿Pero por qué? En las relaciones internacionales generalmente se acepta que un país debe tener un territorio definido, una población y un gobierno que ejerza una única autoridad sobre ambos. Las teorías difieren sobre el último criterio de "naturaleza de país". Debido a que el Congreso de Viena equilibró los intereses en pugna de tantos estados soberanos, cualquier estado nuevo modificaba el Nuevo equilibrio y podía generar otra guerra en el continente. Por ello, la única manera de admitir a algún miembro nuevo en el club de países era que los miembros existentes reconocieran al recién llegado como un estado soberano igual a ellos.

Para decirlo de otro modo: un país no era un país hasta que otros países dijeran que era un país.

La mentalidad del club exclusivo de los miembros creada en el Congreso de Viena sirvió para mantener a Europa en su gran mayoría pacífica durante los siguientes cien años Pero deja al enfoque basado en el riesgo de los bancos en una posición vulnerable.

Reconociendo el problema

La geografía, junto con el producto, la industria y el canal de entrega, es un elemento de medición de riesgo ALD fundamental que utilizan los bancos para evaluar a los clientes y las transacciones. Pero la geografía en realidad es una imagen de un factor más importante: la situación legal. Cuando un banco analiza los lugares geográficos incluidos en una transacción, está mirando realmente a los regímenes legales y regulatorios ALD a los cuales están sujetos las partes involucradas en la transacción. ¿Tuvo el banco emisor que identificar detalladamente a su cliente antes de otorgarle una cuenta? ¿El banco corresponsal en la transacción está autorizado para abrir cuentas a los bancos pantalla? ¿Es el lavado de dinero un delito en el país de donde proviene este cliente? ¿Qué pasa con la corrupción?

Dado que los países asociados con un cliente o transacción son partes tan importantes, los bancos dedican muchos esfuerzos a determinar qué jurisdicciones son de alto riesgo y cuáles no lo son. Pero al organizar las calificaciones de riesgo geográfico, muchos indudablemente adoptan el enfoque del Congreso de Viena — calificando solo a aquellos países que los países existentes consideran que son países.

Este enfoque pasa por alto las realidades vigentes en varios lugares. Un buen ejemplo es la República Turca del Norte de Chipre (TRNC, por sus siglas en inglés). Luego del golpe de 1974 en la República de Chipre, Turquía envió tropas para proteger a la población étnicamente turca que habitaba el tercio norte de la isla. Bajo la protección turca, la parte norte de Chipre establecería un estado separado completo, con presidente, primer ministro, parlamento y poder judicial. A pesar de crear una democracia representativa semipresidencial, la TRNC no es reconocida como país por ningún otro país salvo Turquía.

Debido a que la TRNC no es una nación reconocida, la mayoría de los bancos no la incluye en sus evaluaciones de riesgo geográfico. Esto presenta un problema al antilavado de dinero (ALD). Los clientes o las transacciones generadas desde Nicosia (la ciudad dividida que es la capital tanto de la República de Chipre como de la República Turca del Norte de Chipre) podrían estar sujetos a dos situaciones legales muy diferentes y por ende podría representar distintos riesgos ALD. La República de Chipre es un miembro de la Unión Europea y es signataria de los acuerdos y tratados para impedir el lavado de dinero. Sin embargo, no puede cumplir con ninguna de sus obligaciones en el territorio de la TRNC. La TRNC, por otro lado, se considera a sí misma independiente y no se considerada obligada por los tratados y acuerdos firmados por la República de Chipre. Dado que no está reconocida como un país legítimo, la TRNC no puede ser parte de tratados ni acuerdos que impidan el lavado de dinero.

En efecto, el tercio norte de Chipre es un agujero negro ALD: técnicamente es parte de un país que tiene todos los mecanismos legales para impedir el lavado de dinero, pero no tiene la capacidad para aplicarlos y está representada por un gobierno que no está obligado por tratados o acuerdos porque ningún otro país le reconoce facultades para firmarlos.

Atenuantes de Montevideo

Casi 120 anos después de que el último delegado se fuera de Viena, otra conferencia en el otro lado del mundo acuñó una definición de país más aceptable para el ALD. Según el criterio aplicado en la Convención de Monte-

video, no era necesario el reconocimiento de los otros países. Más allá del territorio, la población y el gobierno, un estado solo necesitaba la capacidad de entrar en relaciones con otros países para poder ser considerado un país en sí mismo.

Para decirlo de otra manera: si parece un país y actúa como un país, es un país, sin importar lo que otros países tengan que decir.

La utilización de la definición de Montevideo como base para la calificación del riesgo geográfico tiene sentido porque resuelve el problema del reconocimiento limitado. Con un territorio y una población definida, un gobierno establecido y la posibilidad de entrar en relaciones con otros países, la TRNC sería incluida. De igual manera serían incluidos otros varios países en todo el mundo que gozan de un reconocimiento limitado.

Ver cuadro complementario para jurisdicciones adicionales no reconocidos o con reconocimiento limitado en el mundo.

Uno de los desafíos de las relaciones internacionales es que no existe un poder supremo para imponer definiciones y enfoques comunes. Así, Teoría Declarativa de Montevideo coexiste actualmente con la Teoría Constitutiva de Viena — cada país es libre de elegir cuál teoría quiere utilizar cuando un territorio nuevo quiere convertirse en miembro del club de países. En realidad, muchos países eligen la teoría más conveniente que se adapte a sus políticas y propósitos.

Los bancos deberían hacer lo mismo.

Max R. Tappeiner, Asesor ALD Global, Royal Bank of Scotland NV., Amsterdam, Holanda. max.r.tappeiner@rbs.com

Las opiniones contenidas en este artículo pertenecen a su autor y no necesariamente representan las opiniones del Royal Bank of Scotland Group.

Otros agujeros negros ALD: Países no reconocidos o con reconocimiento limitado

la República Turca del Norte de Chipre es uno de los varios agujeros negros ALD esparcidos en el mundo. Oficialmente denominados "países con reconocimiento limitado", es más común leer de ellos en la prensa como territorios "separados" o "disputados". Independientemente del nombre, estas áreas representan los mismos riesgos ALD: un gobierno central nominalmente en control de territorio pero autoridad sobre el terreno es impugnada por otro gobierno. En muchos casos, los gobiernos no reconocidos ejercen poderes legítimos como la emisión de pasaportes y el control de fronteras territoriales.

País	Capital	Lugar	Reconocimiento	Historia	Emite Pasaportes	Ejerce Soberanía Territorial
Abkhazia	Suhkumi	Mar Negro / Cáucaso	Rusia, Nicaragua, Venezuela, Nauru	Declaró la independencia de Georgia en 1992	Sí	Sí
Kosovo	Pristina	Sudeste de Europa	71 de los 191 estados miembro de la ONU, incluidos la mayoría pero no todos los miembros de la UE	Declaró la independencia de Serbia en 2008	Sí	Sí
Nagorno-Karabakh	Stepanakert	Cáucaso	Ningún miembro de la ONU reconoce a Nagorno-Karabakh	Declaró la independencia de la Unión Soviética en 1992. Territorio reclamado por Azerbaiján	No	Sí
Palestine	Jerusalem	Este del Mediterráneo	Debido a la naturaleza ambigua de las declaraciones sobre el tema del estado palestino, se estima que entre 115 y 130 países reconocen a Palestina	La Organización de la Liberación de Palestina declaró el estado palestino en 1988 desde Argel	Sí	No
Sahrawi Arab Dem. Rep.	El Aaiún	Noroeste de África	57 países reconocen a la SADR y otros 8 reconocen pero han "congelado" o de otra manera suspendido el reconocimiento hasta que se realice un referéndum sobre la autodeterminación	Con el fin del dominio colonial español, los países vecinos buscaron anexar el territorio de Sahara Occidental. Un movimiento político local declaró la independencia en 1976. Marruecos ocupa la mayor parte del territorio reclamado por la SADR	Sí	Parcial
Somaliland	Hargeisa	Cuerno de África	No está reconocido oficialmente por ningún país, sin embargo, varios países tienen relaciones políticas y no diplomáticas con Somalilandia.	Declaró la independencia de Somalia en 1991 luego del colapso del gobierno somalí durante la Guerra Civil Somalí	Sí	Sí
South Ossetia	Tskhinvali	Cáucaso	Rusia, Nicaragua, Venezuela, Nauru	Declaró la independencia de Georgia en 1991	Sí	Sí
Transnistria (Trans-Dniestr)	Tiraspol	Mar Negro	No reconocido oficialmente por ningún país	Declaró la independencia de Moldova en 1990	Sí	Sí

Combatiendo el lavado de dinero basado en el comercio a mediante asociaciones globales

Investigaciones de Seguridad Interior (Homeland Security Investigations, o HIS, por sus siglas en inglés), el brazo investigativo de la oficina de Control de Inmigraciones y Aduanas de los EE.UU. (ICE, por sus siglas en inglés), ha sido líder en la realización de investigaciones de lavado de dinero basado en el comercio. Debido a su autoridad y acceso únicos a la información comercial como financiera, HSI está posicionado estratégicamente para combatir a las organizaciones criminales que explotan las vulnerabilidades del comercio global y los sistemas financieros.

¿Qué es el lavado de dinero basado en el comercio?

El Lavado de Dinero Basado en el Comercio (LDBC) es una clase de lavado de dinero en la cual los criminales utilizan al sistema de comercio internacional para ocultar los fondos ilegales alterando los documentos de trabajo aduaneros y bancarios, haciéndolos aparecer como legítimos. Desafortunadamente, las vulnerabilidades en el sistema de comercio internacional ofrecen numerosas oportunidades para su explotación. Algunos criminales simplemente dependen del mero volumen del comercio internacional para ocultar sus delitos. Otros utilizan la complejidad de las transacciones de cambio de divisas extranjeras y los diversos instrumentos financieros para ocultar sus actividades fraudulentas. Muchos métodos de fraudes aduaneros tradicionales como la facturación falsa, la sobrefacturación y la subfacturación de comodities a menudo son utilizados para transferir fondos en todo el mundo. Para incrementar el valor de sus fondos ilícitos, los criminales frecuentemente organizan distintos estratos con varios esquemas.

Mercado Negro de Cambio de Pesos

Un ejemplo bien conocido del LDBC, utilizado en gran medida por los carteles de la droga colombianos para repatriar el dinero generado en el tráfico de drogas, es conocido comúnmente como Mercado Negro de Cambio de Pesos (MNCP). El MNCP opera como un sistema financiero de cambio subterráneo utilizado para evadir las obligaciones de conservación de registros requeridas por la Ley de Secreto Bancario (LSB) en los EE.UU., y también para evadir la obligación de reporte bancario, los derechos aduaneros, los impuestos a las ventas y el impuesto a las ganancias de Colombia. El esquema general incluye la compra de productos de exportación de los EE.UU. destinados a Colombia con fondos procedentes de las ventas de drogas ilegales.

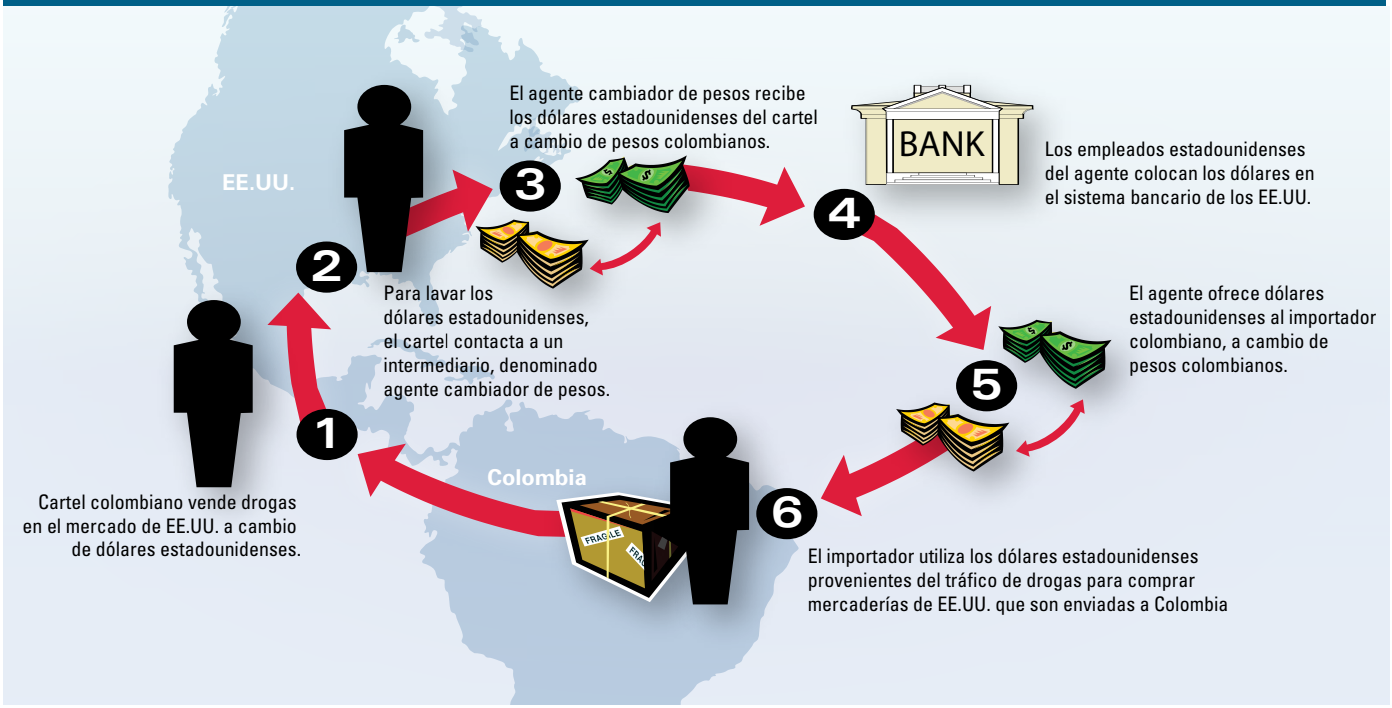
El siguiente escenario muestra cómo un cartel colombiano podría utilizar MNCP para lavar fondos ilícitos. Un cartel colombiano vende cocaína en los EE.UU. y recibe dólares estadounidenses ilegales. El cartel luego contacta a un agente de cambio de pesos colombiano para lavar su dinero. El agente de cambio de pesos arregla el retiro de los fondos ilícitos del cartel y su colocación en instituciones financieras estadounidenses, a menudo a través de depósitos estructurados en varias cuentas bancarias. A continuación, el agente de cambio de pesos contacta a importadores colombianos que quieren importar productos de los EE.UU. y a exportadores de los EE.UU. que exportarán sus productos a Colombia.

Una vez que estas relaciones son establecidas, agente cambiador de pesos utiliza los fondos ilegales ya ingresados en el sistema bancario estadounidense para pagar a los exportadores de los EE.UU. por los embarques a Colombia. Consecuentemente, los fondos ilegales nunca abandonan los EE.UU. El agente cambiador de pesos luego instruye al exportador para que envíe sus productos a un determinado importador colombiano. El importador colombiano recibe las mercaderías y posteriormente le paga al agente cambiador de pesos colombiano en pesos por el embarque. El agente cambiador de pesos luego devuelve los pesos limpios al cartel de la droga. Todos los participantes se benefician con la transacción sea mediante el incremento de sus ventas y/o el cobro de un arancel por su participación. Además, el importador colombiano puede falsificar fácilmente sus facturas reduciendo o evitando los aranceles aduaneros colombianos.

Unidades de transparencia comercial

cuando se habla del LDBC, uno de los principales factores utilizados por los criminales además de la complejidad de la transacción comercial internacional es la idea de que la agencia aduanera solo puede ver un lado de la transacción comercial. Por ejemplo, si un exportador de los EE.UU. envía computadoras por valor de US$1 millón a Brasil, los funcionarios aduaneros estadounidenses no saben qué se informa al ingresar a Brasil. Un

Ejemplo de Lavado de Dinero a través del Comercio Global



Fuente: Control de Inmigración y Aduanas de los EE.UU.

importador brasileño en complicidad con el exportador podría cambiar fácilmente los documentos para reflejar el valor del embarque en US$500.000. Esto le permitiría al importador brasileño justificar un pago reducido de US$500.000 al exportador de los EE.UU., transfiriendo los US$500.000 adicionales a Brasil.

Este ejemplo es un esquema típico del LDBC denominado subvaluación. Al facturar las mercaderías por debajo del valor de mercado, el exportador puede transferir valor al importador. Una vez que el importador vende las mercaderías, recibirá el valor total de los productos. En este ejemplo, dado que el importador solo pagó US$500.000 al exportador, aún le adeuda al exportador US$500.000 porque el verdadero valor del embarque era de US$1 millón. Esta porción de la deuda puede ser cancelada utilizar un mercado bancario paralelo como el MNCP o un esquema similar del Mercado Negro Brasileño denominado *Dolerios*. Sin embargo, si las dos agencias aduaneras de los EE.UU. y Brasil pudieran ver los documentos de la operación comercial de cada una de ellas, la transacción se vuelve evidente, permitiéndole al personal de control legal identificar las transacciones fraudulentas indicadoras de lavado de dinero y otros delitos.

Esta transparencia es la teoría detrás de la creación de la iniciativa de la Unidad de Transparencia Comercial (UTC) de HSI. La UTC es un esfuerzo de colaboración entre HSI, la agencia de Protección de Aduanas y Fronteras de los EE.UU. (CBP, por sus siglas en inglés), el Departamento de Estado y el Departamento del Tesoro. La primera UTC fue creada en Washington D.C. en la sede central de HSI. En ese momento, HSI comenzó identificando a los países que estaban interesados en trabajar en conjunto e intercambiar la información comercial. Actualmente, HSI ha desarrollado trabajos conjuntos con Argentina, Brasil, Colombia, México, Panamá y Paraguay. A través de esas relaciones, HSI y las UTCs extranjeras intercambian información comercial, permitiendo la visibilidad a ambos lados de la transacción comercial.

Las UTCs de HSI conllevan el reconocimiento mundial a la amenaza del lavado de dinero basado en el comercio y los esfuerzos de HIS para combatir y prevenir esta amenaza. Reconocido como el mejor mecanismo para combatir el lavado de dinero basado en el comercio, las UTCs han sido destacadas en varias publicaciones del gobierno de los EE.UU., incluida la *Evaluación Nacional de Amenaza de Lavado de Dinero (The National Money Laundering Threat Assessment)*, las *Estrategias Nacionales de Lavado de Dinero* del Departamento del Tesoro *(National Money Laundering Strategies)* y las *Estrategias Internacionales para el Control de Narcóticos* del Departamento de Estado (International Narcotics Control Strategies).

Utilizando un software especializado y técnicas probadas de investigación los funcionarios pueden analizar la información comercial y financiera para ayudar a identificar las transacciones comerciales y cualquier otra información que no siga los patrones normales de la actividad. Para ayudar a realizar este análisis, HSI ha desarrollado un sistema de computación especializado denominado Sistema de Análisis & Investigación para la Transparencia Comercial *(Data Analysis & Research for Trade Transparency System*, o DARTTS, por sus siglas en inglés). Este programa es utilizado tanto por HSI como por UTC socias extranjeras para ayudar a identificar los indicadores de lavado de dinero, fraude aduanero, contrabando y evasión de aranceles e impuestos.

Al establecer estas asociaciones internacionales, las UTCs ofrecen otro medio para vincular globalmente a las agencias aduaneras y de control legal, ampliando las redes para ayudar a combatir el crimen transna-

cional. En los últimos años, estos esfuerzos conjuntos han identificado e impedido actividades de organizaciones criminales que realizaban esquemas comerciales fraudulentos, MNCP, lavado de dinero, y exportaciones ilegales de productos, resultando en numerosos arrestos y decomisos de millones de dólares en fondos y productos.

Recientes investigaciones exitosas

HSI, como parte del Grupo de Trabajo Conjunto contra el Terrorismo (JTTF, por sus siglas en inglés), inició un caso para investigar la exportación sospechosa de productos electrónicos desde Miami, estado de la Florida, hacia Ciudad del Este, en Paraguay. Ciudad del Este tiene fronteras con Argentina y Brasil, y es parte de una región conocida comúnmente como Triple Frontera. Una de las zonas libres de impuestos más grande del mundo, Ciudad del Este, es también un centro sudamericano de contrabando, productos falsificados armas ilegales y otras actividades ilícitas. En diciembre de 2006, Galería Page, uno de los centros de compras más grandes de Ciudad del Este, fue designado como entidad Especialmente Designada por Terrorismo Global *(Specially Designated Global Terrorist*, o SDGT, por sus siglas en inglés) por la Oficina de Control de Bienes Extranjeros, por sus vínculos con el grupo terrorista Hezbollah. Una vez que un individuo o negocio es designado como SDGT, se les prohíbe a las entidades estadounidenses realizar negocios con la SDGT o, de lo contrario, enfrentan juicios penales.

A medida que la investigación avanzaba, los agentes especiales de HSI y los funcionarios de CBP, junto con los miembros del grupo de trabajo JTTF, establecieron que varias compañías de envío de carga con sede en Miami exportaban ilegalmente productos electrónicos a Galería Page. En su trabajo con los miembros de la UTC en Paraguay para verificar los documentos, los agentes descubrieron que los criminales ocultaban el verdadero destino de los embarques prohibidos utilizando facturas falsas que contenían domicilios falsos y consignatarios finales ficticios en los documentos de exportación. Además, los pagos mediante transferencias electrónicas eran direccionados a través de varios destinos para ocultar su verdadero origen.

Como resultado de la investigación, cuatro individuos y tres compañías de envío de carga con sede en Miami fueron acusados de cargos de conspiración por violar la Ley de Poderes de Emergencia Económica Internacional *(International Emergency Economic Powers Act*, o IEEPA, por sus siglas en inglés) y contrabando de productos electrónicos. Hasta octubre de 2010, tres de los cuatro individuos se habían declarado culpables. Además, como parte de la investigación, se decomisaron más de US$119 millones en productos, principalmente electrónicos de alto valor.

Una segunda investigación de LDBC a gran escala incluyó un esquema de MNCP que operaba en una compañía de juguetes con sede en Los Ángeles. Los fondos procedentes del tráfico de drogas, que aparentemente eran lavados a través de depósitos de dinero en efectivo estructurados, eran utilizados para comprar juguetes de animales rellenos, incluidos osos. Los juguetes posteriormente eran exportados a Colombia para su venta y los pesos colombianos generados por esas ventas eran luego utilizados para su devolución a los traficantes de drogas colombianos.

En julio de 2010, los demandados judicialmente asociados con la compañía de juguetes y la organización de lavado de dinero fueron acusados de cargos que incluían transacciones de estructuración para evitar la obligación de reporte, contrabando de grandes cantidades de dinero en efectivo e intimidación de testigos. Además, la empresa de juguetes fue acusada de conspiración para lavar dinero. Basándose en las acusaciones criminales de estructuración, también se presentó un pedido de decomiso criminal de US$8,6 millones por los valores estructurados.

El uso del comercio como instrumento para lavar ingresos ilícitos es un esquema complejo y en evolución que presentará desafíos a las autoridades de control legal durante décadas. Pero con el desarrollo de la UTC de HSI y sus socios globales, así también como con el constante compromiso demostrado por HSI con la constante expansión del programa, las autoridades de control legal pueden combatir de manera efectiva el mundo en constante cambio del LDBC.

Para obtener información adicional sobre la UTC o el LDBC, por favor contar al Jefe de la Unidad UTC en TTU.TTU@dhs.gov.

Jennifer Eisner, jefa de sección, Unidad de Transparencia Comercial, Investigaciones de Seguridad Interior, Washington, D.C., EE.UU.Jennifer.Eisner@dhs.gov

Indicadores de señales de alerta de lavado de dinero basado en el comercio

- Pagos a un vendedor realizados por terceros no relacionados
- Pagos a un vender realizados mediante transferencias electrónicas de terceros no relacionados
- Pagos a un vendedor mediante cheques, giros bancarios, giros postales de dinero o cheques de viajero de terceros no relacionados
- Sospecha o conocimiento del uso de compañías pantalla y cuentas relacionadas
- Patrones no explicados, repetidos o inusuales de actividades de transferencias
- Reporte falso: como la clasificación incorrecta de commodity, sobrevaluación o subvaluación de commodity
- Transacciones giratorias: la importación y exportación repetida del mismo commodity de alto valor
- Los commodities que se venden con se condicen con el negocio en cuestión
- Rutas de embarque o puntos de transbordo inusuales que no tienen sentido económico
- Envoltura inconsistente con el commodity o el método de envío
- Doble facturación
- Diferencias entre el valor facturado del commodity y el valor de mercado
- El pago de las mercaderías es superior o inferior al valor conocido de mercado
- El tamaño del embarque es inconsistente con el volumen promedio del negocio

La Ley de Cumplimiento de Impuesto sobre Cuenta Extranjera: Estar atentos para ver sus efectos

Los EE.UU. tienen una larga historia de tratar de detener la evasión fiscal por parte de sus ciudadanos y residentes que utilizan cuentas extranjeras solo con éxito limitado. Una industria offshore altamente sofisticada, integrada por profesionales financieros, banqueros, agentes, corredores, proveedores de servicios corporativos, abogados especializados en impuestos, contadores y administradores de fideicomisos, asesora y ayuda a los estadounidenses para abrir cuentas offshore y ocultar bienes a fin de evadir impuestos y a los acreedores en sus jurisdicciones de origen.[1]

El Congreso ha estimado que cada año los EE.UU. pierden cerca de US$100.000 millones en ingresos por impuestos a causa de los abusos offshore.[2] El 18 de Marzo de 2010, el Congreso aprobó una ley amplia denominada Ley de Cumplimiento de Impuestos sobre Cuenta Extranjera *(Foreign Account Tax Compliance Act*, o FATCA, por sus siglas en inglés) en un esfuerzo por combatir la evasión de impuestos offshore por parte de "personas de los EE.UU.", incluidos los ciudadanos de los EE.UU. o los residentes en los EE.UU., las compañías que no cotizan en bolsas, las sociedades y las sucesiones. Si bien la mayoría de sus efectos no se producirán hasta después del 31 de Diciembre de 2012, la FATCA tiene un efecto tan oneroso sobre las instituciones financieras extranjeras (IFEs) que optan por hacer negocios con "personas de los EE.UU." que estas instituciones deben empezar a prepararse para su aplicación lo más pronto posible.

En general, crea un complejo régimen de retenciones diseñado para sancionar a las IFEs y las entidades extranjeras que se niegan a entregar las identidades de sus clientes estadounidenses. Si bien ha habido muchas investigaciones sobre abusos impositivos offshore, la Ley es consecuencia de dos importantes escándalos impositivos recientes, uno de ellos involucró al LGT Bank de Liechtenstein y otro al UBS en Suiza. También se produce en un momento en que los EE.UU. han otorgado importantes subsidios al sector bancario y cuando el país, a causa de un gran déficit, tiene una gran necesidad de contar con más ingresos por impuestos. Este artículo señalará algunos antecedentes sobre la ley actual, describirá brevemente la FATCA, y presentará algunas preguntas y temas de interés pendientes e indicará algunas medidas que las IFEs pueden tomar inmediatamente para asegurarse que están preparadas para cumplir con la Ley en 2013.

Antecedentes sobre los intentos para detener la evasión fiscal

En 2001, el gobierno de los EE.UU. estableció el Programa de Intermediario Calificado *(Qualified Intermediary Program*, o QIP, por sus siglas en inglés), la ley relacionada con la evasión fiscal. Alentó (pero no obligó) a las IFEs, indicadas en la ley como Intermediarios Calificados (ICs), a que firmaran un acuerdo con el IRS para actuar como agentes de retención de los EE.UU. y cumplir con las obligaciones de retención fijadas en la ley impositiva de los EE.UU. para sus clientes de los EE.UU. Cada IC está obligado a descifrar la naturaleza y monto de la fuente de ingresos de sus clientes estadounidenses, establecer si los clientes son elegibles para obtener los beneficios otorgados mediante tratados según el país de residencia de los clientes y luego calcular e informar los montos correspondientes al IRS. El QIP también las obliga a aplicar procedimientos de conozca a su cliente (CSC) para verificar y documentar al dueño beneficiario de cada una de sus cuentas, y cada IC debe utilizar auditores externos para asegurar el cumplimiento con las normas. Sin embargo, como parte de este acuerdo, los ICs no están obligados a informar las identidades o nacionalidades de sus clientes. Los ICs se opusieron enfáticamente a hacer eso, no solo porque le abría la puerta a la competencia por parte de las instituciones financieras de los EE.UU., sino también porque afectaba sus políticas sobre secreto bancario.[3]

El QIP ha tenido sus deficiencias. En primer lugar, el QIP es voluntario y por lo tanto hay muchas IFEs que no participan en el programa. Debido a ello, hay una gran cantidad de menores retenciones u otorgamientos indebidos de exenciones impositivas y beneficios impositivos otorgados por tratados. En segundo lugar, la posibilidad de las personas de los EE.UU. para establecer corporaciones offshore, fideicomisos y fundaciones (a veces alentadas por los ICs) les permite a algunos contribuyentes estadounidenses recibir indebidamente exenciones o evadir impuestos simplemente porque tienen sus fondos en estos vehículos. Las reglas actuales del CSC, en su gran mayoría, no requieren que las IFEs obtengan información sobre los dueños beneficiarios de estas entidades. Además, en muchos casos en que hubo ICs no se realizaron investigaciones de fraude o actos ilegales.[4]

Los EE.UU. no son los únicos que están tratando de detener la evasión fiscal. Varias organizaciones multinacionales como la Organización para la Cooperación y el Desarrollo Económico (OECD, por sus siglas en inglés) y la Directiva de Ahorros de la Unión Europea han tratado de detener la evasión impositiva a nivel internacional y de promover los intercambios de información impositiva. La OECD ha podido reducir la lista de "paraísos fiscales no cooperadores" de manera considerable durante la última década. Sin embargo, todavía hay países que tienen restricciones importantes sobre la divulgación de la información bancaria. Muchos de estos países promulgan leyes que les permiten a los no residentes constituir compañías, fideicomisos, fundaciones y otras entidades legales a bajos costos y mantener sus bienes en cuentas financieras protegidas por leyes de secreto que son aplicadas con multas criminales y civiles.[5]

[1]Subcomité Permanente de Investigaciones del Senado de los EE.UU., *Los Abusos de los Paraísos Fiscales: Los Facilitadores, Las Herramientas y el Secreto (Tax Haven Abuses:The Enablers,The Tools and Secrecy)*, (1 de Agosto de 2006): 1.

[2]Senador Levin, Registro Parlamentario del Senado, S1745: *Ley de Contratación (Hire Act)* 18 de Marzo de 2010.

[3]Subcomité Permanente de Investigaciones del Senado de los EE.UU., *Bancos de Paraísos Fiscales y Cumplimiento Fiscal de los EE.UU. (Tax Haven Banks and U.S. Tax Compliance)* 17 de Julio de 2008, 21–26.

[4]Oficina de Responsabilidad Gubernamental de los EE.UU. (U.S. Government Accountability Office), *El Programa de Intermediarios Calificados Brinda Cierta Seguridad de que los Impuestos sobre los Inversores Extranjeros Son Retenidos e Informados, pero Puede Ser Mejorado*, Diciembre de 2007.

[5]Id at 26–36.

En su última publicación, el Foro Global sobre Transparencia e Intercambio de Información con Fines Impositivos indicó:

"Cada vez más frecuentemente, la gente trabaja hoy en más de una jurisdicción, las corporaciones multinacionales manejas sus temas en redes de subsidiarias y compañías holding cada vez más complejas, las cuentas de bancos extranjeros pueden abrirse en cuestión de minutos en la web, y los fideicomisos pueden crearse para administrar los bienes familiares para los hijos y nietos en docenas de distintas jurisdicciones. Ya no es posible que ninguna jurisdicción se base solamente en la información disponible dentro de sus propias fronteras para aplicar sus propias leyes".[6]

Una breve descripción de la FATCA

A continuación se detalla un breve resumen de la FATCA pero no incluye todos los detalles y disposiciones. La FATCA extiende y amplía significativamente las obligaciones de reporte para ciertas entidades extranjeras con relación a las "personas de los EE.UU.". Las entidades extranjeras ya no pueden ocultar la identidad de sus clientes estadounidenses como podían hacer en el QIP. Los EE.UU. contarán con las IFEs y las entidades extranjeras no financieras (NFFEs, por sus siglas en inglés) que tengan clientes estadounidenses para brindar información sobre su identidad a fin de ayudarles a tratar de detener la evasión fiscal en los EE.UU. Si no lo hacen, deben dar por terminadas las relaciones con sus clientes estadounidenses u optar por pagar una multa del 30% de la retención sobre los "pagos que debieron ser retenidos" a los fines de esta Ley, incluir el ingreso FDAP de fuente estadounidense (p.e., intereses, dividendos, etc.) y los ingresos brutos de la venta de la propiedad que pueda generar intereses o dividendos de fuentes estadounidenses.[7]

La definición de IFEs ha sido ampliada para incluir no solamente a los bancos sino también a instituciones como las firmas de corretaje, las compañías de inversión y los *hedge funds*, así también como a sus afiliadas. Las IFEs también pueden optar por ser consideradas como instituciones financieras estadounidenses y presentar el Formulario 1099 del IRS por cada titular de cuenta estadounidense o tienen la opción de celebrar un acuerdo con el IRS para aplicar procedimientos que identifiquen a los titulares de cuentas estadounidenses. Esto requiere que se reporten anualmente el nombre, domicilio, número de identificación tributaria (TIN, por sus siglas en inglés), número de cuenta, saldo de la cuenta, ingresos brutos y extracciones brutas de cada cuenta.[8]

La IFE también debe retener el 30% de cualquier "pago intermediario" (pass thru payments) realizado a titulares de cuentas contumaces que no deseen cumplir con la divulgación de la información.[9] Cuando una ley extranjera impida el reporte de la información, la IFE tratará de obtener una autorización válida y efectiva de dicha ley por parte de los titulares de cuentas. Si dicha autorización no fuere obtenida, entonces la cuenta deberá ser cerrada. Las IFEs no participantes que no firmen el acuerdo, enfrentan la retención del impuesto del 30% sobre todos los "pagos que pudieren ser retenidos".[10]

En la guía preliminar del IRS, Aviso 2010-60, ciertas IFEs han sido excluidas del cumplimiento con la FATCA. Entre las exclusiones se encuentran las compañías de seguros que emiten seguros sin valor en efectivo (p.e., seguros de propiedad y accidente y de vida a plazo); los establecimientos de compañías durante los primeros 24 meses desde el inicio del desarrollo del negocio; y los planes de retiro auspiciados por un empleador no estadounidense sin ningún participante o beneficiario estadounidense.[11]

La NFFE es definida como cualquier otra entidad que no está incluida dentro de la definición de IFE, incluidos los negocios que operan en forma privada, sin cotizar en bolsas, las firmas de servicios profesionales, los fideicomisos extranjeros y las asociaciones extranjeras.[12] A fin de que la NFFE evite el 30% del impuesto sobre la retención, debe extar exenta del impuesto; ser una empresa que cotice en bolsa (o una afiliada de una empresa que cotice en bolsa); certificar que no tiene gran cantidad de propietarios estadounidenses (aquellos que directa o indirectamente son dueños de más del 10% de la entidad); o debe informar el nombre, domicilio y TIN de cada propietario sustancial estadounidense a un agente de retención o al IRS.[13]

También existen nuevas obligaciones de reporte para cualquier individuo que tenga un interés en un bien extranjero y se aplican penalidades a aquellos que no cumplan con la disposición. Estas obligaciones son complementarias de las actuales obligaciones FBAR.[14]

Además, se establece una exención minima para todos los titulares de cuentas estadounidenses con cuentas de depósito de menos de US$50.000.[15] El IRS ha indicado que la FATCA requerirá el reporte electrónico y que creará nuevos formularios y acuerdos.[16] Aún quedan preguntas sin repuestas y el Departamento del Tesoro preparará guías para una mayor implementación factible.

Preguntas y temas de interés

La FATCA definitivamente les dificulta a las "personas de los EE.UU." la posibilidad de ocultar los bienes en cuentas offshore. Sin dudas, es un gran paso hacia la creación de

[6]OECD (2010), *Tax Co-operation 2010: Towards a Level Playing Field*, OECD Publishing, http://dx.doi.org/10.1787/taxcoop-2010-en.
[7]Código Sec. 1473(1)(A)(i). Cualquier pago de interés (incluido cualquier emisión original de descuento), dividendos, rentas, salarios, sueldos, premios, rentas anuales, compensaciones, remuneraciones, emolumentos y otros ingresos, valores, ganancias fijos o determinables anual o periódicamente, si dicho pago proviene de fuentes dentro de los EE.UU.
[8]Código Sec. 1471(c).
[9]Código Sec. 1471(b)(1)(D). Incluye cualquier pago que se atribuya a un pago que deba ser retenido.
[10]Código Sec.1471(b)(1)(F).
[11]Aviso IRS 2010-60.
[12]Código Sec.1472(d).
[13]Código Sec.1472.
[14]Kevin E. Packman, Esq. y Mauricio D. Rivero, Esq., "The Foreign Account Tax Compliance Act Taxpayers Face More Disclosures and Potential Penalties", *Journal of Accountancy* (Agosto 2010): 1. Report of Foreign Bank and Financial Accounts which must be filed by U.S. persons having a financial interest in or signature authority or other authority over any financial account in a foreign country if the aggregate value of these accounts exceeds $10,000 at any time during the calendar year.
[15]Código Sec.1471(d)(1)(B).
[16]Aviso IRS2010-60.

un mundo financiero global más transparente y responsable. También puede establecer un estándar para que el resto del mundo lo adopte a fin de evitar la evasión fiscal en los demás países.

Pero surgen muchas preguntas. Primero, ¿vale la pena el costo de una Ley como ésta, que es tan gravosa tanto para el IRS como para la comunidad financiera internacional? Según el Comité Conjunto sobre Impuestos, se estima que la FATCA solo recuperará US$8.700 millones en impuestos de los EE.UU. durante los próximos 10 años.[17] Esto está muy lejos de los US$100.000 millones estimados por el Congreso como pérdida anual a causa de la evasión fiscal. ¿A qué se debe la diferencia? ¿Es una sobreestimación del Congreso, una subestimación del Comité Conjunto sobre Impuestos, o es que la FATCA solo va a evitar una pequeña porción de la evasión fiscal en los EE.UU.?

Sin dudas, los costos de la implementación de la FATCA van a ser soportados por las IFEs. Los riesgos inherentes, las complejidades de la creación de sistemas tecnológicos amplios y los desafíos legales, especialmente en las situaciones en donde la FATCA entre en conflicto con las leyes locales de las IFEs, son una enorme carga para las IFEs. La Federación Bancaria Europea y el Instituto de Banqueros Internacionales, en sus comentarios públicos al IRS, expresaron que muchas instituciones grandes han estimado de manera conservadora que les costará, en promedio, alrededor de US$10 revisar cada cuenta e identificar correctamente si se trata de una cuenta cuyo titular beneficiario es una "persona de los EE.UU." o no. Muchas de estas instituciones tienen entre 30 y 50 millones de cuentas.[18] Existe cierta preocupación en la comunidad internacional de que la FATCA sea una solución que se aplique a todas las instituciones por igual, lo cual demasiado abarcador para las IFEs, algunas de las cuales tienen muy pocos clientes estadounidenses. Algunas argumentan que la FATCA debería estar más basada en el riesgo, reducir las obligaciones de documentar, reporte y retención de aquellas entidades, cuentas y pagos que sean de bajo riesgo.

Aunque será costoso, la mayoría de las instituciones más grandes cumplirán con la FATCA porque tienen suficientes recursos para pagar la asistencia legal, contable y tecnológica para implementar la ley. Son las instituciones más pequeñas las que podrían sufrir debido a los elevados costos y la falta de personal con conocimientos de las leyes impositivas estadounidenses. Incluso es difícil para muchos abogados estadounidenses tratar de desentrañar y comprender el Código de Rentas Internas de los EE.UU. ¿Entonces qué podemos esperar de una institución pequeña en un país extranjero cuyos empleados no hablen inglés para poder conocer y tener los medios para cumplir con las leyes impositivas de los EE.UU.? ¿Hará la FATCA que las instituciones más pequeñas que hayan tenido que deshacerse de los clientes estadounidenses o retirarse de invertir en los mercados estadounidenses sean adquiridas por otras instituciones?

La versión original de la FATCA incluye disposiciones para imponer obligaciones de reporte sobre los "asesores materiales" incluidos los abogados y contadores que ganen más de US$100.000 al año colaborando en la creación directa o indirecta o en la adquisición de un interés en una entidad extranjera.[19] Esta norma no fue incluida en la versión final de la ley. Por lo tanto, no solamente fueron excluidos de la ley, sino que está claro que estos proveedores de servicios profesionales se beneficiarán enormemente con la FATCA ya que serán necesarios para asistir a las IFEs y las NFFEs de todo el mundo para conocer y cumplir con las disposiciones de la ley. ¿Es posible que su omisión en la ley pudiera regresar y volverse en contra de los EE.UU.?

Los ciudadanos estadounidenses que viven en el exterior sin dudas temen no solamente los costos que las IFEs les pudieren aplicar, sino también el riesgo de que sus cuentas financieras pudieran ser cerradas. Algunas IFEs tal vez no estén en condiciones de poder cumplir con las obligaciones de cumplimiento para conservarlos como clientes. La discriminación contra los estadounidenses que viven en el exterior también podría darse como consecuencia de la ley. De acuerdo con los comentarios presentados por los Ciudadanos Estadounidenses en el Exterior:

"Los ciudadanos estadounidenses que residen en el exterior se encuentran en el medio del fuego cruzado y son los claros perdedores — imposibilitados de mantener relaciones bancarias en los Estados Unidos, imposibilitados de tratar de tener relaciones bancarias en el exterior pero aún así, necesitando servicios bancarios para pagar impuestos en los EE.UU., invertir fondos y simplemente vivir en un mundo moderno".[20]

Medidas a tomarse ahora mismo

Aunque el Departamento del Tesoro aún no ha emitido las guías finales, hay algunas medidas que las IFEs deberían tomar inmediatamente. Primero de todo, el Departamento del Tesoro está pidiéndole al público comentarios sobre la FATCA, por lo cual, si una IFE o una organización tienen comentarios, éste es el momento de enviarlos al Departamento del Tesoro.[21] Además, cada IFE debería crear un grupo de trabajo interno sobre la FATCA a fin de elaborar un conocimiento claro de la ley y evaluar la situación actual con relación a las cuentas mantenidas por "personas de los EE.UU.". El grupo de trabajo debería incluir personal legal, impositivo, ALD y tecnológico. Este grupo de trabajo debe identificar a todas las partes afectadas por la ley y educar a sus empleados sobre la FATCA, especialmente al personal de cumplimiento y a los gerentes de relaciones o a cualquiera que interactúe con el público. Debería establecerse cuántos clientes estadounidenses tiene la IFE y qué información ya está en su base de datos con relación a la identidad de sus clientes estadounidenses. Luego, el grupo de trabajo debería elaborar una lista de actividades a realizar para su desarrollador de la aplicación para que haya una base de datos electrónica disponible en 2013. Cada IFE también debería determinar la mejor manera de que sus clientes estadounidenses conozcan a la FATCA. Si cada organización espera a las regulaciones finales del Departamento del Tesoro, podría ser demasiado tarde para lograr el cumplimiento en 2013.

Diane Eisinger, J.D., LL.M; CFP®, CAMS, vicepresidenta, Spectrum Advisors, Inc. Williamsburg, VA, EE.UU., Diane6022@gmail.com

[17]Comité Conjunto sobre Informe Impositivo t, JCX-5-10, 23 de Febrero de 2010.
[18]Federación Europea Bancaria y el Instituto de Banqueros Internacionales, *Comentarios sobre Aviso 2010-6- Providing Preliminary Guidance on FATCA*, 12 de Noviembre de 2010, en 3.
[19]Dirk. J.J. Suringa, Esq., U.S. *Withholding and Reporting Requirements for Payments of U.S. Source Income to Foreign Persons*, 19 de Enero de 2010.
[20]American Citizens Abroad, *Comments on Foreign Account Tax Compliance Act (FATCA) Provisions Incorporated in the Hiring Incentives to Restore Employment Act (HIRE*, 14 de Junio de 2010).
[21]Aviso IRS 2010-60

Capítulo de Australia

En noviembre de 2010, el Capítulo de Australia emprendió un proceso modificado de de nominación y elección de una nueva junta directiva en la Reunión Anual General (AGM, por sus siglas en inglés). El proceso de nominación y elección es un requisito de acuerdo con el Manual de los Capítulos que les otorga a todos los miembros de los capítulos el derecho a emitir una opinión sobre la composición de la nueva junta ejecutiva y la opción de ser miembros de la misma. Éste ciertamente es el caso del Capítulo de Australia. Aunque la AGM misma se realizó el 23 de noviembre, el proceso de nominación y elección se completó durante todo el mes de noviembre. La oficina central de ACAMS colaboró con el capítulo en la realización del proceso de promoción del proceso de nominación.

Los resultados de la elección mostraron que hay un interés cada vez mayor no solo en los trabajos de la junta sino en el capítulo en general. Los nuevos quince integrantes de la junta ejecutiva son: Guy Boyd (co-presidente); Aub Chapman (co-presidente); Erum Khan (co-secretario); Gavin Coles (co-secretario); Julie Beesley (co-tesorera); Stuart Hansen (co-tesorero y co-programador, Nueva Zelanda); Tim Land (co-membresía); Phil O'Connell (co-membresía); Paddy Oliver (co-comunicaciones); Crispin Yuen (co-comunicaciones); Bill Brown (co-programación, Melbourne); Graham Gorrie (co-programación, Sydney); Alex Tan (co-programación, Nueva Zelanda); Dr Hugh McDermott (co-programación, webseminarios); Brett Webber (co-programación, webseminarios). Los miembros de la junta directiva con sede en Nueva Zelanda, Stuart, Phil y Alex, tienen el apoyo de los miembros del Grupo de Trabajo de Nueva Zelanda, Gary Hughes y Tim Morrison. Al ampliar la cantidad de miembros de la junta, junto con carteras de la junta más concentradas, la junta ejecutiva tiene como objetivo ofrecer actividades más específicas a los miembros del capítulo.

La AGM se realizó en la oficina de KPMG en Sydney con conexión mediante videoconferencia con Melbourne. Los asistentes escucharon a Lindsay Chan del Grupo Asia/Pacífico sobre Lavado de Dinero (Secretaría de APG), seguida de Aub Chapman (co-presidente) quien en nombre de la junta saliente, brindó un informe sobre los tres primeros años del Capítulo.

Lindsay ofreció un informe amplio sobre las opiniones del APG sobre los temas ALD emergentes en la región Asia-Pacífico para los próximos dos o tres años. Después de un informe sobre los miembros del APG, Lindsay se concentró en varios temas. Primero, los temas de lavado de dinero de interés en la región, que incluyen: corrupción, fraude, paraísos fiscales, talas ilegales y tráfico de personas. Las debilidades regionales fueron el segundo tema de la reunión. Lindsay se refirió a los vacíos en los regímenes legales, la falta de concientización sobre los estándares del GAFI y la falta de recursos. El tema final se vinculó al proceso de revisión en curso del GAFI sobre la aplicación de las 40+9 Recomendaciones. Este tema desencadenó una animada discusión, especialmente sobre el tema de la propiedad beneficiaria contenido en la Recomendación 5.

El informe de Aub se refirió a la historia de nuestro capítulo desde su creación en 2007. Al hacer mención a los miembros de la junta, Aub agradeció a todos los miembros anteriores y actuales de la junta por sus contribuciones. Aub hizo un breve resumen de las actividades de los miembros realizadas durante los últimos tres años, con un agradecimiento a todos los oradores invitados y a los auspiciantes. Finalmente, Aub habló acerca del futuro del capítulo y su dirección en la región de Australia.

Puede obtenerse una copia de la presentación de Lindsay y del informe de Aub en la página de Internet del Capítulo.

La junta desea agradecer a los socios de KMPG por facilitar las oficinas y por su excelente hospitalidad.

En Nueva Zelanda, ACAMS dirigió dos sesiones muy informativas tanto en Auckland como en Wellington durante noviembre. Entre 60 y 45 miembros de la industria asistieron a cada una de las respectivas sesiones. El director y gerente de operaciones de la Agencia del Crimen Organizado y Financiero de NZ (OFCANZ, por sus siglas en inglés) realizó una presentación. La exposición dio un panorama de esta nueva agencia de control legal, su trabajo, como se integraron al ámbito del control legal en NZ y algunos casos de estudio relacionados con el ALD. Los casos de estudio destacaron los riesgos en NZ presentados por los agentes de constitución de compañías y por las oficinas de servicios monetarios. Los representantes de los tres supervisores ALD de Nueva Zelanda asistieron a las sesiones. La junta desea agradecer a los socios de PWC por facilitar las instalaciones y por la excelente hospitalidad recibida.

En la foto de I a D: Director de la Junta, Alex Tan; Presentadores en Auckland de OFCANZ, Malcolm Burgess y Brett Kane; Miembro del grupo, Gary Hughes

En el futuro el capítulo dirigirá sus esfuerzos a incrementar sus miembros, relacionarse con la industria y los reguladores, con el objetivo de liderar la organización profesional ALD/CFT en la región.

La Universidad de Nueva Gales del Sur (UNSW, por sus siglas en inglés) es una socio oficial de ACAMS y la Faculta de Derecho ofrecerá nuevamente durante 2011 un curso titulado "Antilavado de Dinero y Fondos Procedentes del Crimen: Leyes y Contramedidas". ACAMS considerará que los estudiantes que completen exitosamente este curso y se incorporen como miembros de ACAMS (o ya lo sean) cumplirán con su criterio de pre-calificacion para dar el examen de Especialista Certificado en Antilavado de Dinero Certificado (CAMS). Este curso también califica para créditos CE para los miembros de ACAMS que sean Certificados CAMS. Para obtener más detalles sobre el curso ALD de la UNSW y sobre nuestro capítulo, visite nuestra página en el sitio www.acams.org.au.

Capítulo de Nueva York

¡El Capítulo de Nueva York de ACAMS se enorgullece de darles la bienvenida a sus dos más recientes miembros de la junta ejecutiva! Hal Crawford de Brown Brothers Harriman & Co y Meryl Lutsky de la Oficina del Fiscal General del Estado de Nueva York fueron seleccionados para integrar la junta ejecutiva en la reunión de directores realizada en diciembre de 2010.

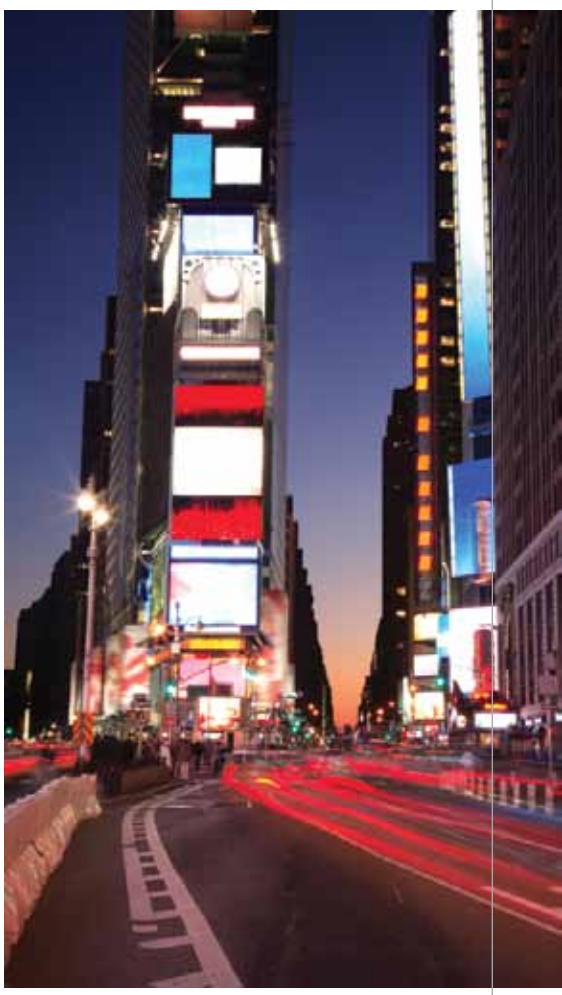
Crawford es el director global de antilavado de dinero y subdirector de cumplimiento de Brown Brothers Harriman & Co., el banco asociado más antiguo y más grande de los Estados Unidos de América. Es responsable de la supervisión y dirección de los programas ALD y de sanciones internacionales de la firma y participa en varias actividades gerenciales senior diseñadas para mejorar las prácticas de control de administración del riesgo regulatorio a nivel general de la firma. Tiene más de veinte años de experiencia en los servicios financieros globales, asesoramiento y supervisión de bancos nacionales. Su experiencia en el sector bancario incluye haber sido suboficial regional para la prevención del lavado de dinero y director de inteligencia financiera en el UBS Investment Bank en Nueva York, director nacional para la diligencia debida reforzada en US Trust Company de Nueva York y oficial de cumplimiento en Mid-Hudson Savings Bank. Trabajó varios años en la Práctica de Servicios de Riesgo Regulatorio de Arthur Andersen, y fue examinador bancario nacional de la Oficina de Contralor de la Moneda (OCC, por sus siglas en inglés). Crawford ha colaborado durante mucho tiempo con el Capítulo de Nueva York y organizó su evento sobre pagos móviles y banca electrónica en Julio de 2010 en la oficina central de Brown Brothers Harriman & Co en Nueva York.

Lutsky ha sido la directora de la unidad de lavado de dinero de la Oficina del Fiscal Federal de Nueva York y del Grupo de Trabajo sobre Fondos Procedentes de Delitos de Nueva York desde 2004. Estas unidades investigan y llevan a juicio las actividades de lavado de dinero y su conducta criminal asociada, así también como las violaciones a las leyes bancaria y tributaria. Para investigar estos complejos delitos de manera más efectiva y creativa, ha formado un grupo de trabajo integrados por fiscales federales y estatales, oficiales de control legal y reguladores. Entre otros casos, recientemente ha investigado varias operaciones de fraude en varios estados cuyos delitos incluían el robo de identidad, lavado de dinero, fraude con tarjetas de crédito, fraude bancario y fraude con transferencias electrónicas.

Lutsky también es muy active en la educación y capacitación de las entidades financieras sobre cómo proteger a sus instituciones frente al fraude financiero. Participa en reuniones de grupos de trabajo regionales en todo el estado y se reúne con las instituciones individualmente para analizar sus exposiciones al riesgo y controles específicos. También ha realizado exposiciones sobre lavado de dinero y otros temas relacionados en varios seminarios y conferencias, incluida la Conferencia Antilavado de Dinero de ACAMS en Las Vegas, la Conferencia Antilavado de Dinero de la Costa Oeste en San Francisco, el Simposio financiero de HIFCA en Nueva York, la Conferencia MAGLOCLE en Columbus, y la Conferencia sobre Lavado de Dinero de ABA/ABA en Washington D.C. Por su trabajo, Lutsky ha recibido el Premio al Profesional ALD del Año en la Conferencia Antilavado de Dinero de ACAMS realizada en Las Vegas en Septiembre de 2010 y su mención fue incluida en la edición anterior de *ACAMS Today*.

Entre los miembros que se reincorporaron a la junta directiva se incluyen a los copresidentes Barry Koch de JP Morgan Chase y Vasilios Chrisos de Macquarie Bank y a los miembros de la junta Robert Goecks de EGRIS LLC, Allen Love de TD Bank, Denise Wright de RBC Capital Markets, David Chenkin de Zeichner Ellman & Krause LLP, James Stubbs de Citi, Dan Wager de la HIFCA de Nueva York, Erika Giovanetti de Morgan Stanley Smith Barney y Martin Feuer de Zurich Financial Services.

El Capítulo de Nueva York de ACAMS ha planificado muchos eventos de aprendizaje interesantes e informativos para el 2011. El evento de febrero sobre Ciberdelitos presentó al escritor James Verini, autor del artículo *El Gran Cibergolpe (The Great Cyberheist)*, publicado en la edición del 10 de Noviembre de 2010 de *The Sunday New York Times Magazine*. Si está interesado en ingresar al capítulo o asistir a un evento, por favor visite nuestra página web en www.acams.org/ACAMS/ACAMS/Communities/Chapters/NewYork. ¡Los eventos son gratuitos para los miembros activos del capítulo! También puede contactarnos por correo electrónico a acamsnewyorkchapter@gmail.com.



Capítulo del Norte de California de ACAMS

¡Hemos crecido mucho y rápido!

La cantidad de miembros se ha incrementado hasta llegar a los 120 miembros del capítulo desde nuestro lanzamiento el 23 de Junio de 2010 en el Marine Memorial en San Francisco. El objetivo de la junta ejecutiva es aumentar el número de miembros hasta llegar a los 150 durante nuestra campaña de membresía de 2011 organizando programas de aprendizaje importantes y emocionantes eventos sociales en la comunidad ALD del Norte de California para ayudar a los miembros a profundizar y ampliar sus conocimientos.

Cambios en la junta

El Capítulo del Norte de California de ACAMS le da la bienvenida a las últimas incorporaciones y despide a otros miembros de la junta ejecutiva.

En Junio de 2010, la secretaria del capítulo, Eileen Monsurate y la codirectora de programación, Natalie Ware presentaron lamentablemente sus renuncias a la junta. Las extrañamos y les deseamos éxitos en sus nuevos emprendimientos.

En Julio de 2010, le dimos la bienvenida a nuestro nuevo codirector de membresía, Bob Kenny de FinCEN.

En Noviembre de 2010, recibimos a nuestra nueva secretaria del capítulo, Erin Balbanian de Google, a la cosecretaria, Elaine Laye, Asesora Legal de la FDIC y al codirector de programación r Shawndra Rutledge, del Bank of the West.

En Enero de 2011, luego de mudarse al área de la bahía, le dimos la bienvenida a nuestro nuevo codirector de comunicaciones, Brian Stoeckert, ex codirector de comunicaciones de la junta ejecutiva del Capítulo del Sur de California.

Will Voorhees y Mikhail Reider-Gordon

Eventos de aprendiza y novedades del programa

6/10/10 Mundos virtuales y e-divisas

el 6 de Octubre de 2010, el Capítulo del Norte de California de ACAMS organizó su primer evento de aprendizaje de su año inaugural con *La Tecnología del Lavado: mundos virtuales, teléfonos celulares, e-divisas — los nuevos bancos del mundo & las nuevas ALD*, presentado por Mikhail Reider-Gordon, director administrador de Litigios y Forense de Capstone Advisory Group, LLC. Más de 30 personas asistieron a este entusiasta evento auspiciado y organizado por el Silicon Valley Bank en San José. No solo los asistentes recibieron dos créditos 2 CAMS, sino que también recibieron muchos conocimientos relacionados directamente con la reciente propuesta de FinCEN de cambiar la definición, bajo la LSB, de los programas de valor acumulado.

Una de las tendencias más novedosas y menos reguladas es el uso del dinero virtual utilizado para cometer crímenes, incluido el asesinato a sueldo. El dinero virtual se ha convertido en un gran negocio. En Hong Kong, la tarjeta Octopus es una tarjeta inteligente anónima de valor acumulado recargable utilizada por el 95% de la población, que genera más de 11 millones de transacciones diarias por valor de más de HK$100 millones (equivalente a US$12,8 millones). A esta industria no regulada actualmente se tiene acceso y es utilizada por dispositivos tales como teléfonos celulares y relojes pulsera — e incluso muñequeras de niños.

Las conclusiones finales de este evento de aprendizaje son que los bancos teniendo menos importancia por las plataformas móviles recientemente surgidas y las monedas móviles. Las compañías de telecomunicaciones están cada vez más brindando servicios financieros asociados con los bancos "de ladrillo y cemento". Al utilizar un teléfono celular prepagado o un teléfono celular regular, la gente puede realizar la mayoría de sus transacciones diarias por teléfono, a menudo frustrando los esfuerzos de monitoreo realizados por las instituciones financieras.

9/12/10 Recolección de juguetes para entregarlos a los niños

por favor lea nuestro comunicado de prensa en la Página Web de nuestro Capítulo.

Nuestro evento de fin de año fue una cocktailera en el Restaurant Bocanova en la hermosa plaza Jack London. Varios miembros asistieron a este evento social gratuito y probaron varios de los sabrosos aperitivos y postres. Organizamos una recolección de juguetes para beneficiar a nuestra comunidad local durante las fiestas. Agradecemos el apoyo de los miembros y el de nuestro auspiciantes Alacra.

27/1/11 Primer evento conjunto de aprendizaje en la historia de ACAMS

Los Capítulos del Sur de California y del Norte de California reunieron sus fuerzas para presentar el webseminario *Conociendo a los Paraísos Fiscales Offshore y El Impacto de las Nuevas Leyes sobre Transparencia Fiscal sobre las IFs.*

La vuelta al mundo: Mejores prácticas para cumplir con la OFAC

La directora de programación Perla Ortiz y el codirector de programación Shawndra Rutledge están preparando un seminario organizado para analizar los últimos cambios en las sanciones de la OFAC, las obligaciones y las mejores prácticas con suficiente detalle como para brindarles a los asistentes el conocimiento necesario para volver a sus organizaciones y revisar y/o mejorar sus programas OFAC.

Además, como valor agregado, la sesión dedicará entre quince y veinte minutos al análisis del impacto sobre los cambios regulatorios en México. La modificación ha estado en vigencia desde hace algunos meses — ¿ha tenido algún impacto sobre la manera en que hacemos negocios? ¿Ha habido algún impacto mensurable sobre los esfuerzos antilavado de dinero o el movimiento del dinero en efectivo ilícito?

Manténgase en contacto

Deseamos mantenerlos informados sobre los próximos eventos y las novedades del capítulo. Si todavía no se ha unido a nuestro Grupo en LinkedIn por favor ingrese al sitio y agregue el Capítulo del Norte de California de ACAMS. También puede encontrar información sobre los futuros eventos en la página web de nuestro Capítulo. www.acams.org/ACAMS/ACAMS/Communities/Chapters/NorthernCalifornia

Sandra Copas, PI, CFE, directora de comunicaciones del Capítulo del Norte de California de ACAMS,scopas@copas-inc.com

Excelente asistencia al segundo evento de aprendizaje del Capítulo Canadiense

Un panel de discusión que generó gran reflexión sobre los temas de cumplimiento ALD fue el centro del segundo evento de aprendizaje del Capítulo Canadiense de ACAMS.

Estuvieron presentes alrededor de 130 participantes asistieron al almuerzo organizado el 5 de octubre de 2010. El almuerzo se organizó luego del éxito obtenido por el primer evento de aprendizaje del capítulo y la presentación del comisionado asistente Mike Cabana de la Real Policía Montada Canadiense fue bien recibida.

El almuerzo contó con la presencia de algunos de los principales CAMLOs de Canadá. Fue gentilmente organizado por Anne Toal, CAMLO de Great-West Life, y Kirsten Lamertz-Harcourt, también Great-West Life, en el edificio de Canada Life en Toronto. El almuerzo fue auspiciado por Lexis Nexis.

Los organizadores del evento querían brindarles a los participantes las perspectivas prácticas sobre los temas que pueden enfrentar a diario. Para convertir a este evento en especialmente importante, recurrieron a CAMLOs representantes de varios sectores.

El panel fue moderado por Barbara Cox, vicepresidente y oficial jefe antilavado de dinero del BMO Financial Group. Los panelistas fueron Karim Rajwani, CAMLO de RBC representando al sector bancario; Richard Hogeveen, CAMLO de Manulife Financial representando a las aseguradoras de vida; y Derek McMillan, Director de Cumplimiento ALD de Western Union representando a los NSMs y las uniones de crédito.

Los temas de discusión incluyeron:

- Las nuevas tendencias en el reporte de operaciones sospechosas, incluida la evasión fiscal, la corrupción y el tráfico de personas.
- Cómo controlar la calidad de los ROSs.
- El enfoque del examen de FINTRAC, la unidad de inteligencia financiera de Canadá.
- Los desafíos para cumplir los requisitos de las sanciones.
- Cómo puede la función ALD agregar valor a la empresa a nivel general de la misma.
- Las mejores prácticas en el monitoreo de transacciones.

El Capítulo de Canadá agradece el intenso trabajo de los siguientes miembros de su junta ejecutiva que encabezaron la organización de este evento: Richard Hogeveen, oficial jefe ALD responsable del programa ALD/CFT de Manulife Financial; Tim McNeil, gerente senior, Unidad de Inteligencia Financiera del Bank of Montreal; Karim Rajwani, CAMLO de RBC; Garry Clement, presidente y CEO de Clement Advisory Group; y Kata Martínez, gerente de desarrollo de capítulos y enlace de los grupos de trabajo de ACAMS.

Capítulo del Gran Boston

En apoyo de la dedicación de la junta ejecutiva del Capítulo del Gran Boston de ACAMS para brindarles a los miembros oportunidades de aprendizaje que sean de interés local y nacional, la junta ejecutiva organizó una sesión especial a fin de 2010. Esta sesión se concentró en la planificación de valiosas oportunidades de aprendizaje dinámico y contactos con colegas para el nuevo año. Los eventos brindarán a los miembros del capítulo un equilibrio de temas, presentadores y foros a lo largo de 2011. El formato de los evento planificados incluye una combinación de reuniones con presentaciones formales reuniones sociales en la tarde exclusivas para los miembros del capítulos, mesas redondas de discusión dirigidas por varios expertos en distintos temas y una oportunidad de capacitación durante todo un día. Los temas varías desde los temas candentes del control legal hasta los tópicos relacionados bancos y desde la perspectiva de los EE.UU. hasta el estado del antilavado de dinero en América Latina.

El año se inició en febrero con un caso de estudio que ya había sido anticipado, presentado por los miembros del Grupo de Trabajo de Lavado de Dinero de la Agencia de Control de Narcóticos (DEA, por sus siglas en inglés). John Grella de la DEA y Ryan Talbot de Investigaciones Criminales del Servicio de Rentas Internas (IRS, por sus siglas en inglés) hicieron su presentación sobre el mercado negro de cambio de pesos, el aspecto de la estructuración del lavado de dinero y las órdenes de decomiso.

Marzo trae la muy esperada primavera y los primeros eventos sociales del Capítulo del Gran Boston de ACAMS. Una reunión por la tarde en el lugar favorito de Beantown brinda la oportunidad a los miembros del capítulo de tener un gran intercambio de ideas, charlas abiertas y de hacer contacto con otros profesionales.

Si está interesado en asistir a estos eventos, por favor asóciese a nuestro capítulo visitando nuestra página web en http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/GreaterBoston/Default.aspx. Si desea realizar alguna consulta sobre el capítulo o si tiene alguna idea o sugerencia para los eventos, por favor póngase en contacto con alguno de los miembros de la junta ejecutiva indicados en el sitio web o envíe un mensaje de correo electrónico a acams-boston@gmail.com.

Inauguración del subcapítulo de Edmonton de ACAMS (integrante del Capítulo de Canadá de ACAMS)

Los especialistas antilavado de dinero (ALD) del área de Edmonton y un miembro del grupo de trabajo regional de Calgary de ACAMS se aventuraron en probablemente uno de los días más fríos del año para asistir al primer evento del Subcapítulo de ACAMS celebrado en la Compañía Cervecera de Amber. A pesar de que uno de los calefactores no funcionaba, todos disfrutaron del encuentro con otros especialistas ALD.

La tarde contó con una breve presentación por parte de nuestro auspiciante del evento, Brad Chafer, ejecutivo de cuenta de la región oeste, de Lexis Nexis. La presentación se focalizó en la solución de administración de identidad de clientes Bridger Insight XG,m diseñada para asistir en el cumplimiento ALD. Lexis Nexis fue muy generoso con su auspicio promocional, el que incluyó la entrega de tres copias de la publicación *A Guide to Canadian Money Laundering Legislation* (Una Guía sobre la Legislación Canadiense sobre Lavado de Dinero), escrita por Terence D. Hall.

A continuación de la presentación realizada por Lexis Nexis se realizó una visita a la cervecería y hubo una degustación de cervezas. El evento transcurrió agradablemente, todos parecieron disfrutar el poder conocer la herramienta "Bridger Insight", las historias de los maestros cerveceros sobre lavado de dinero en la industria de los bares y la corrupción gubernamental, así también como la oportunidad de probar distintas clases de cerveza.

Hemos recibido comentarios favorables sobre el evento y estamos planeando nuestro próximo evento para Febrero/Marzo de 2011.

Capítulo de las Carolinas

El Capítulo de las Carolinas regresó a la Ciudad Reina para su primera reunión de 2011. Bank of America en la ciudad de Charlotte esta vez fue el lugar donde el presidente del capítulo, Bill Fox dio la bienvenida al director ejecutivo asociado de Investigaciones de Seguridad Interior, Control de Inmigración y Aduanas (ICE, por sus siglas en inglés), James Dinkins. Dinkins, quien dirige la segunda agencia más importante de investigaciones criminales de los Estados Unidos, expuso ante el grupo sobre la misión de ICE y más específicamente el problema creciente del contrabando y tráfico de personas y el rol que las iniciativas ALD juegan en la detección y disuasión de este trágico delito. Dinkins informó sobre las estadísticas y compartió estudios de casos de traficantes de víctimas que eran extranjeros ilegales, mujeres y niños y las asociaciones públicas/privadas que en muchos casos son responsables de llevar a esta gente ante la justicia. Más de 100 miembros del capítulo asistieron para escuchar la presentación y brindar sus opiniones sobre las tendencias ALD en este campo. "El tráfico de personas y sus costos financieros y sociales no pueden ser ignorados por las instituciones financieras y ACAMS está ofreciendo un valioso recursos educando a los profesionales ALD para ayudar a combatir este crimen", dijo el recientemente elegido co-presidente del capítulo Rob Goldfinger.

Esperamos contar con más eventos importantes en el Capítulo de las Carolinas en los próximos meses y brindarles eventos de capacitación de más calidad y contacto entre colegas en la región.

Para obtener más información sobre el Capítulo de las Carolinas de ACAMS, por favor contactar a Rob Goldfinger en RGoldfinger@sightspan.com. O, para conocer cómo participar en éste o cualquier otro capítulo, por favor contactar a Kata Martínez, gerente de desarrollo de capítulos de ACAMS, en cmartinez@acams.org.

Por favor, visite la página web del Capítulo de las Carolinas en http://www.acams.org/Chapters/Carolinas.aspx.

Capítulo del Sur de California

El Capítulo de ACAMS del Sur de California cerró el 2010 con un evento de aprendizaje en la sede de la municipalidad al que asistieron representantes de las autoridades federales de control legal y se preparó para el 2011 con una novedad en ACAMS con el primer evento de aprendizaje presentado en forma conjunta con otro capítulo.

El 2 de diciembre de 2010, el capítulo presentó "Financiamiento del Terrorismo en el Sur de California: Casos Recientes y Tendencias". La reunión se realizó en el Elk's Lodge en San Gabriel, California, y fue seguida de una recepción con motivo de las fiestas de fin de año abierta a todos los profesionales de ACAMS. El panel incluyó a representantes de la Oficina Federal de investigaciones, la Oficina del Fiscal Federal de los Estados Unidos, la División de Investigaciones Criminales del Servicio de Rentas Internas y Control de Aduanas e Inmigración de los Estados Unidos.

Los panelistas analizaron diversos casos de métodos de financiamiento del terrorismo, incluido el lavado de dinero a través del comercio, las transferencias electrónicas internacionales mediante terceros intermediarios, las transferencias de fondos sin una conexión lógica con el remitente o beneficiario y los fondos procedentes de las ventas de productos falsificados que son contrabandeados en grandes volúmenes de dinero en efectivo a través de Asia y México.

En un foro abierto con el panel, la audiencia de más de 70 asistentes participaron en una sesión de preguntas y respuestas que superó el ámbito del evento. El panel analizó temas que incluyeron cómo utilizan los agentes de control legal los Reportes de Operaciones Sospechosas (ROSs) remitidos a FinCEN, la naturaleza del intenso manejo de dinero en efectivo en el Medio Oriente, las compañías pantalla utilizadas para transferir fondos, el tráfico de personas, el contrabando de grandes cantidades de dinero en efectivo en el aeropuerto de Los Ángeles y el valor subyacentes de los documentos respaldatorios de los ROSs en un juicio por lavado de dinero.

Lo que es más importante, el panel destacó la importancia y la efectividad de crear relaciones en la comunidad local de delitos financieros. Uno de los panelistas dio varios ejemplos de cómo la relación con las instituciones financieras ayudó enormemente en un decomiso federal. Además, uno de los panelistas recomendó a los profesionales antilavado de dinero que lean la segunda eidición de *Lavado de Dinero: Una guía para los Investigadores Criminales (Money Laundering: A Guide for Criminal Investigators)*, segunda edición, de John Madinger, que ofrece una perspectiva amplia sobre los delitos financieros, los métodos, casos de estudio y las leyes aplicables.

Para comenzar con el programa de 2011, el capítulo ha organizado el primer evento de aprendizaje publicitado y desarrollado con otro capítulo. El 27 de enero de 2011, el Capítulo del Sur de California de ACAMS y el Capítulo del Norte de California de ACAMS, junto con DLA Piper LLP, una importante firma internacional de abogados, presentaron un webseminarios sobre "Conociendo los Paraísos Fiscales Offshore y el Impacto de las Nuevas Leyes de Transparencia Impositva para las Instituciones Financieras". El webseminario de dos horas de duración otorgó a los asistentes dos (2) créditos CAMS a los miembros de ambos capítulos. Los oradores invitados incluyeron a Alan Granwell, socio, DLA Piper LLP, Bruce Zagaris, socio, Berliner, Corcoran & Rowe LLP y James Dowling, director, Dowling Advisory Group. Mikhail Reider-Gordon, director administrador de Capstone Advisory Group, LLC fue el moderador.

Finalmente, en diciembre, el miembro de la junta ejecutiva Brian Stoeckert fue designado por John Byrne, vicepresidente ejecutivo de ACAMS, Presidente del recientemente creado Comité Directivo de los Capítulos de ACAMS, quien colaborará con los Capítulos nuevos y ya existentes de ACAMS.

Capítulo de Sudáfrica

Nuestra misión es "apoyar la misión internacional de ACAMS, mejorar el conocimiento de los especialistas ALD/CTF locales, y brindar un vehículo a través del cual nuestros miembros locales puedan conectarse y mejorar el nivel del conocimiento y efectividad ALD/CTF".

Capítulos de Sudáfrica de ACAMS — novedades y actualizaciones

Antecedentes del capítulo e inauguración:

El capítulo de Sudáfrica de ACAMS fue oficialmente inaugurado en Johannesburgo el 3 de Noviembre de 2010 y auspiciado por PWC. La junta de Sudáfrica se reunió inicialmente durante Febrero de 2010 y comenzó e proceso y análisis para inaugurar el capítulo a fin de 2010. Con la asistencia de diversos capítulo, ACAMS de EE.UU. y una tremenda cantidad de trabajo y esfuerzo por parte de toda la junta, el lanzamiento fue un éxito enorme. También tuvimos el gusto de tener al vicepresidente ejecutivo de ACAMS John Byrne y a José Lewis, el gerente regional para África, Asia y el Medio Oriente en la inauguración. Desde una perspectiva sudafricana, tuvimos a Murray Michel, director del Centro de Inteligencia Financiera y a varios representantes del área de control legal, el sector bancario internacional la junta independiente de auditores regulatorios, la asociación de casinos de Sudáfrica, académicos de varias universidades, el banco de la reserva sudafricana, firmas de auditoría incluidas KPMG, Deloitte, E&Y y PWC, la autoridad judicial nacional, el servicio de rentas sudafricano, compañías de seguros y muchos más.

Principales mensajes:

John y Murray dieron los mensajes más importantes durante la inauguración, a la que asistieron aproximadamente sesenta delegados. A continuación se detalla un extracto de los comentarios principales:

- Cómo cuadra ACAMS dentro del ámbito local y el impacto que podría tener.
- La amenaza global de las drogas, el terrorismo, el tráfico de personal, el contrabando de armas, el fraude y la corrupción.
- El flujo de fondos ilegales en el ámbito global a través de varias instituciones.
- El gobierno sudafricano y el compromiso de los participantes en la lucha contra el lavado de dinero y los delitos relacionados.
- La interdependencia y la cooperación requeridas entre los centros privados y público en la lucha contra el crimen organizado.
- Mejora de la facultades de identificación, monitoreo y enjuiciamiento.
- La inauguración del capítulo de Sudáfrica de ACAMS es un hito en la lucha contra el crimen en Sudáfrica y se logrará un mayor cumplimiento ALD en todos los negocios a través del proceso de certificación CAMS.
- El intercambio de las mejores prácticas internacionales y una interacción intensiva con el GAFI.
- ACAMS Sudáfrica será el vehículo para atraer a los expertos ALD de varias y diversas industrias.

Crecimiento del capítulo desde la inauguración:

El Capítulo de Sudáfrica de ACAMS tiene el agrado de anunciar que las solicitudes de membresía recibidas desde la inauguración el 3 de Noviembre de 2010 hasta fin de Enero de 2011 han llegado a 73. Los miembros de la junta se han visto colmados con pedidos de membresía e información adicional. El capítulo también está comprometido a organizar eventos de aprendizaje y de encuentros con colegas durante el año en Johannesburgo y en Ciudad del Cabo — consulte el sitio web del capítulo para obtener más información. Algunas de las novedades recientes incluyen una conferencia africana de ACAMS a ser organizada en Johannesburgo durante Julio de 2011.

Para obtener más información sobre el capítulo de Sudáfrica de ACAMS incluyendo detalles sobre su misión, la composición de la junta, los próximos eventos e información general, por favor visite su página web en at http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/SouthAfrica/Default.aspx o envíe un mensaje de correo electrónico a acamssouthafricachapter@fcrmc.co.za

Chris Steyn, director de comunicaciones, Capítulo de Sudáfrica de ACAMS

Murray Michel, director del Centro de Inteligencia Financiera

John J. Byrne, ACAMS vicepresidente ejecutivo

Capítulo de la Capital de los EE.UU.

El Capítulo de la Capital de los EE.UU. terminó el año con un concurrido evento de fin de año que fue el escenario para presentar el calendario del Capítulo para el 2011. El capítulo está concentrado en la preparación de mejores eventos de aprendizaje con múltiples sesiones para este año.

"Hemos tenido excelentes eventos de aprendizaje durante el año pasado que han tocado temas de importancia para nuestros miembros", dijo Joe Soniat, copresidente del capítulo. "Los eventos de aprendizaje anteriores incluyendo las tendencias del control legal ALD y los temas emergentes, investigaciones criminales y entrevistas con reguladores y autoridades de control legal. Hemos realizado una encuesta entre nuestros miembros y de acuerdo con sus respuestas, vamos a volver con más detalle sobre estos temas. También vamos a incrementar nuestros eventos de capacitación para los negocios de servicios monetarios (NSMs)".

Durante la primera mitad de 2011, el capítulo tiene planeado organizar una sesión de capacitación de tres horas de duración para los NSMs y las instituciones financieras que tienen relaciones comerciales con los NSMs. Todavía no se completó la lista de oradores, pero las sesiones incluirán un panorama general de los NSMs, un repaso de las obligaciones regulatorias de la industria, y las maneras de administrar el riesgo y desarrollar relaciones efectivas entre los NSMs y las instituciones financieras.

El capítulo también está planificando una sesión de un día de duración con representantes del control legal que ofrecerá un panorama general de las tendencias emergentes, casos de estudio y analizará los últimos riesgos y tendencias en el ALD y el CTF. "El capítulo está trabajando estrechamente con la Unidad de Investigaciones Especiales, Narcóticos y Lavado de Dinero del Departamento de Policía del Condado de Fairfax, Virginia, para desarrollar el programa", dijo John Byrne, copresidente del capítulo. "Esperamos ofrecerles un día de sesiones muy interesantes y de muy buena calidad".

Como con todos los eventos del capítulo, la asistencia a estos eventos será gratuita para los miembros del Capítulo de la Capital de EE.UU. Más adelante daremos más información sobre los próximos eventos.

Para ayudar a los miembros a desarrollar sus contactos con los representantes de cumplimiento, el capítulo también llevará a cabo seis eventos sociales este año. En respuesta a los pedidos de los miembros, el lugar para la reunión de las *happy hours* rotará entre Washington, D.C. y Virginia.

El capítulo desea darle la bienvenida a la junta a Don Temple, director de Forensic Advisory Services de KPMG, LLP. Don trae más de 25 años de experiencia en el campo de la Ley de Secreto Bancario y el antilavado de dinero. Su extensa experiencia práctica en las áreas de las investigaciones financieras incluye investigaciones sobre impuestos federales, fraude financiero, diligencia debida y antilavado de dinero.

El capítulo también desea agradecer a Mónica MacGregor por sus servicios a la dirección de membresía del Capítulo de la Capital de los EE.UU. Mónica deja la junta después de dos años. Ella es una de los miembros fundadores del capítulo y ha formado parte de la junta desde su creación.

El Capítulo de Richmond

El Capítulo de Richmond (Virginia) continuó creciendo durante el último trimestre. Su crecimiento aumentó cuando una estación local de televisión invitó a los miembros de la junta del capítulo Elaine Yancey y Joe Soniat a participar en una entrevista en cámara. Joe y Elaine aprovecharon la oportunidad para analizar ACAMS, el Capítulo de Richmond, los esfuerzos antilavado de dinero, lo común que es el problema del lavado de dinero y qué buscan los investigadores para descubrirlo. La entrevista, emitida inicialmente el 8 de Noviembre, fue recogida luego por una agencia nacional de noticias. Tanto Joe como Elaine dijeron que la entrevista ante las cámaras fue una experiencia interesante. A fin de Noviembre el Capítulo de Richmond había crecido sustancialmente con miembros tanto del sector público como del privado.

El 9 de Diciembre el capítulo organizó un evento con motivo de las fiestas de fin de año en el Eurasia Café & Wine, el que incluyó invitaciones con bebidas y aperitivos para los miembros. Esta reunión brindó otra oportunidad para que los miembros socialicen y se conozcan. El Capítulo también aprovechó la ocasión para mostrar su apoyo al Banco Central de Alimentos de Virginia, una valiosa causa comunitaria.

Cerca de fin de año, la junta se reunió para realizar la planificación y organización de eventos para el nuevo año, la cual incluyó varias conferencias de aprendizaje y eventos sociales. El capítulo tiene planeado continuar con su práctica de atraer a importantes profesionales de la industria para que expongan en sus eventos. La Junta del Capítulo de Richmond desea agradecer a aquellos que ya se han convertido en miembros e invita a los profesionales de la industria que viven las áreas de Richmond y sus alrededores que todavía no lo han hecho, a que formen parte del Capítulo. La membresía al Capítulo es una manera costo-eficiente de obtener créditos para la recertificación CAMS, recibir conocimientos diarios útiles y desarrollar valiosos contactos en la industria.

JUNTA DEL CAPÍTULO DE RICHMOND

R. Joe Soniat, Copresidente
Elaine R. Yancey, Copresidente
Elizabeth Vega (Lisa), Secretaria
D. Scott Bailey, Cosecretario
Donna Kitchen, Tesorera
Donna Thrift, Cotesorera
Charlie George, Director de Membresía
Diane Eisinger, Codirectora de Membresía
Fallon Teufert, Director de Programación
Dr. Gurpreet Dhillon, Codirector de Programación
Amy Wotapka, Directora de Comunicaciones
Dr. Thomas J. Burns, Codirector de Comunicaciones

Capítulo de Chicago

En su compromiso constante para brindar educación continua, el Capítulo de Chicago de la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS) organizó un evento de aprendizaje el 10 de Diciembre de 2010 para sus miembros. El tema del evento fue ayudar a mejorar un proceso de monitoreo de listas de advertencia, reducir las falsas alarmas y atender los desafíos asociados con el monitoreo y adaptación antilavado de dinero (ALD). Henry Balani, CAMS, director gerente del Grupo de Servicios Estratégicos de Accuity y Gregory LeMond, CAMS, gerente senior de Crowe Horwath LLP fueron los presentadores del evento. Ambos oradores brindaron excelentes guías y sugerencias para mejorar las eficiencias del monitoreo y las mejores prácticas para lograr una mayor adherencia a los estándares ALD actuales.

Balani dio consejos prácticos y específicos sobre cómo reducir la cantidad de falsas alarmas en el proceso de monitoreo de sanciones. Al definir y ampliar los criterios fundamentales como las clases de entidades, las fuentes, las señales, el procesamiento de las reglas y las falsas alarmas y las falsas eliminaciones, la presentación de Balani cubrió el amplio espectro de los elementos básicos del monitoreo de sanciones. Además, Balani compartió valiosas opiniones ofreciendo sugerencias de mejores prácticas para aplicar en el monitoreo de anomalías, la información de SWIFT, y los patrones de riesgo. LeMond analizó los desafíos asociados con la adaptación específica del programa de monitoreo ALD de transacciones e indicó los pasos específicos sobre cómo atender estos desafíos. Al presentar un análisis comparativo detallado de las condiciones y parámetros del monitoreo de transacciones dentro de un programa ALD estándar, LeMond pudo destacar las claves de la elaboración exitosa de las soluciones de monitoreo. El intercambio de preguntas y respuestas entre los oradores y los asistentes fue animado, particularmente dada la importancia y el impacto del material.

Henry Balani de Accuity y Gregory LeMond de Crowe Horwath LLC

El Capítulo de Chicago también organizó un evento de aprendizaje en febrero y contó con un panel de discusión integrado por tres oradores en el que se analizó la presentación efectiva de los Reportes de Operaciones Sospechosas. Varios eventos que cubren una amplia gama de temas ALD ya están siendo planificados, y serán presentados durante el semestre hasta junio de 2011. Para obtener más información sobre los eventos pasados y futuros, por favor visite el sitio del Capítulo de Chicago en: http://www.acams.org/ACAMS/ACAMS/Communities/Chapters/Chicago/Default.aspx.

Departamento de Operaciones de ACAMS

ACAMS Today tuvo la oportunidad de conversar con Ericka Araujo, coordinadora de soporte comercial de ACAMS. Araujo es el enlace con la oficina de ACAMS en Asia. Las actividades diarias de Araujo incluyen colaborar con los servicios a los miembros en la elaboración y aplicación de las políticas y procedimientos de los servicios a los miembros para asegurar la satisfacción consistente del servicio al cliente y procesar las solicitudes de certificación/recertificación.

Araujo nación en Des Moines, Iowa y se mudó a Miami en 2007. Antes de ingresar a ACAMS, Araujo trabajó en Wells Fargo Home Mortgage en West Des Moines, Iowa, como Asistente Administradora/Administrativa de MAC, donde se ocupaba de la prestación de los servicios a los miembros y colaboraba con el director de operaciones.

Araujo tiene un título asociado en Administración de Negocios del Colegio de la Comunidad del Área de Des Moines y actualmente está preparándose para completar si carrera de bachiller en Administración de Negocios.

ACAMS Today: ¿Cuál ha sido la mayor mejora en la Asociación en los últimos tres años?

Ericka Araujo: En los últimos tres años he visto un crecimiento tremendo en la cantidad de miembros. Como resultado de este crecimiento extraordinario, ACAMS constantemente está buscando maneras de brindarles a sus miembros excelentes servicios, capacitación destacada y por sobre todo, ser una plataforma de contacto para la comunidad ALD. Una de las mejoras más significativas ha sido la creación de más capítulos y la actualización del sitio web.

AT: ¿Qué parte de su trabajo es la que más satisfacciones le da?

EA: Asistir a nuestros miembros de ACAMS para ayudarles a convertirse en CAMS certificados.

AT: ¿Cuál es la parte favorita para usted de las conferencias de ACAMS?

EA: Tengo la oportunidad de trabajar en el sector de inscripción durante las conferencias y esto es una ventaja para mí porque me da la posibilidad de ser una de las primeras personas en conocer a los asistentes. Esto me permite ponerle un rostro al nombre de un miembro al que pude haber ayudado por teléfono o por correo electrónico. También me gusta asistir a los eventos sociales y ver la interacción de unos miembros con otros.

AT: ¿Adónde ve a ACAMS en los próximos cinco años?

EA: En el primer plano. ACAMS seguirá estando al frente de la capacitación en el campo del antilavado de dinero y seguirá creciendo exponencialmente.

SIGHTSPAN®

Navigation for Business Information®

AML/CTF Functional and Technical Expertise

Banking | Brokerage | MSB | Prepaid | Government

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

SightSpan, Inc. USA
Corporate Headquarters
PO Box 4023
Mooresville, NC 28117
United States of America
Phone: (704) 663 0074
Fax: (704) 664 2807

SightSpan, Inc. Singapore
UOB Plaza 1, 80
Raffles Place
Singapore, 048624
Singapore
Phone: +65 6248 4688
Fax: +65 6248 4531

SightSpan, Inc.
New York Office
5 Penn Plaza
19th Floor
New York, NY 10001
United States of America
Phone: +01 212 849 6841

www.sightspan.com