

ACAMS TODAY

La Revista Para los Profesionales en el Campo Antilavado de Dinero

RECONOCIMIENTO *a la Clase* DE 2014



Carol Stabile
Artículo del Año



Brian Arrington
Artículo del Año



Clayton Byford
Artículo del Año

2014 GANADORES DE LOS PREMIOS



Kevin Anderson
*Voluntario Al Gillum
del Año*



Chuck Taylor
*Profesional del Año
de ALD*



Michael McDonald
Premio Pioneer de ALD



Éric Lachapelle
*Capítulo del Año
de Montreal*



DICIEMBRE 2014-FEBRERO 2015
VOL. 14 NO. 1

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

www.ACAMS.org
www.ACAMSToday.org

MEASURE, UNDERSTAND & EXPLAIN YOUR MONEY LAUNDERING RISKS

Help your institution:

- Effectively detect financial crime patterns and spot red flags
- Mitigate risk and regulatory scrutiny by filling in the gaps in your detection and prevention controls
- Save time and expense with comprehensive automation and updates
- Clearly communicate risk through standardized scoring and automated reporting

**For information and to set up a product demo, contact
Tanya Montoya at tmontoya@acams.org.**

ELEVATING KNOW YOUR CUSTOMER TO NEW HEIGHTS

Reliable, Actionable Intelligence

At Booz Allen Hamilton, our Financial Crimes Management Services Team has leveraged capabilities and expertise in working with the intelligence community, national defense and law enforcement. The result is the power to discover each customer's potential risk.

- Ask better questions of customers to reduce your exposure to regulatory action
- Reduce the cost of your AML/financial crimes program while building a scalable workforce
- Improve the accuracy of your investigations to create sustainable operations

To thrive in business today, you need the power to know your customer in more depth. You need to determine the true nature of the relationships between your company and your customer. Together, we work with you to ensure your business takes the right steps for the long view.

To learn how Booz Allen can help you, contact Warren Zafrin, Vice President, Financial Crimes Management, at (917) 305-8019 or zafrin_warren@bah.com.

www.boozallen.com/commercial



ACAMS[®]TODAY

VICEPRESIDENTE EJECUTIVO *John J. Byrne, CAMS*

JEFA DE REDACCIÓN *Karla Monterrosa-Yancey, CAMS*

ACAMS Today, la premiada revista, 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 City Tower
80 Southwest 8th Street, Suite 2350
Miami, FL, 33130

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

| EDICIÓN Y DISEÑO |

ASISTENTE EDITORIAL *Alexa Serrano*

DISEÑADORA GRÁFICA *Victoria Racine*

| GRUPO DE TRABAJO EDITORIAL |

PRESIDENTA *Debbie Hitzeroth, CAMS*

Kevin Anderson, CAMS

Brian Arrington, CAMS

Edwin (Ed) Beemer, CAMS

Cindy Choi

Dilip K. Chowdhary, CAMS

Charles Falciglia, CAMS

Aaron Fox

Tom Garry, CAMS

Robert Goldfinger, CAMS

Jennifer Hanley-Giersch, CAMS

Carolina Rivas, CAMS

Eric Sohn, CAMS

Joe Soniat, CAMS *Joe Soniat, CAMS*



Ganador de los 2014 premios de oro y de plata



Otorgado por el Academy of
Interactive and Visual Arts

Ganador del 2014 Charlie Award



Otorgado por el
Florida Magazine Association

| PERSONAL SENIOR |

OFICIAL EJECUTIVO EN JEFE *Ted Weissberg, CAMS*

OFICIAL FINANCIERO EN JEFE *Ari House, CAMS*

DIRECTORA GLOBAL DE CONFERENCIAS Y CAPACITACIÓN *Eva Bender, CAMS*

JEFA DE ASIA *Hue Dang, CAMS*

DIRECTOR DE VENTAS *Geoffrey Fone*

DIRECTORA DE MARKETING *Kourtney McCarty, CAMS*

DIRECTOR DE OPERACIONES *Joseph Yerant*

| REPRESENTANTES REGIONALES Y DE VENTAS |

VICEPRESIDENTE SENIOR DE DESARROLLO DE NEGOCIOS *Geoffrey Chunowitz, CAMS*

JEFA DEL CARIBE *Denise Enriquez*

JEFA DE AMÉRICA LATINA *Sonia Leon*

JEFE DE ÁFRICA & ORIENTE MEDIO *Jose Victor Lewis*

| CONSEJO DIRECTIVO |

PRESIDENTE *Rick A. Small, CAMS*

Luciano J. Astroga, CAMS

Robert Curry, CAMS

William J. Fox

Peter Hazelwood

María de Lourdes Jiménez

William D. Langford

Karim Rajwani, CAMS

Anna M. Rentschler, CAMS

Anthony Luis Rodriguez, CAMS, CPA

Nancy Saur, CAMS, FICA

Markus E. Schulz

Daniel Soto, CAMS

| ASESORES ESPECIALES PARA EL CONSEJO DIRECTIVO |

Samar Baasiri, CAMS

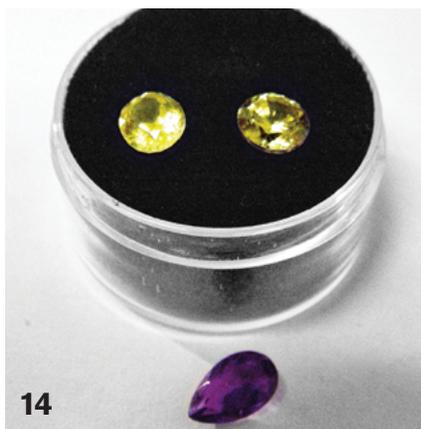
Susan J. Galli, CAMS

Vasilios P. Chrisos, CAMS

David Clark, CAMS

ACAMS[®] | Asociación de
Especialistas Certificados
en Antilavado de Dinero[®]

Contenido



14



18



28

De la editora 8

Noticias de los miembros 10

Carta del vicepresidente ejecutivo 12

**Diamantes:
El mejor amigo del criminal** ... 14

¿Qué es lo que atrae a los blanqueadores de dinero a las piedras y metales preciosos?



Dos componentes cruciales en la lucha contra la trata de personas 18

Las instituciones financieras están en una buena posición para detectar la trata de personas, ¿pero están recibiendo suficiente entrenamiento y educación sobre este tema?

Las empresas de servicios monetarios—¿Víctimas del enfoque basado en el riesgo? 20

¿Si se cierra cuentas de MSB es esto realmente una solución a la lucha contra la delincuencia o es que solo está alimentando el fuego?

La trama del Mercado Negro de Cambio de Pesos: El pasado, el presente y el futuro probable 24

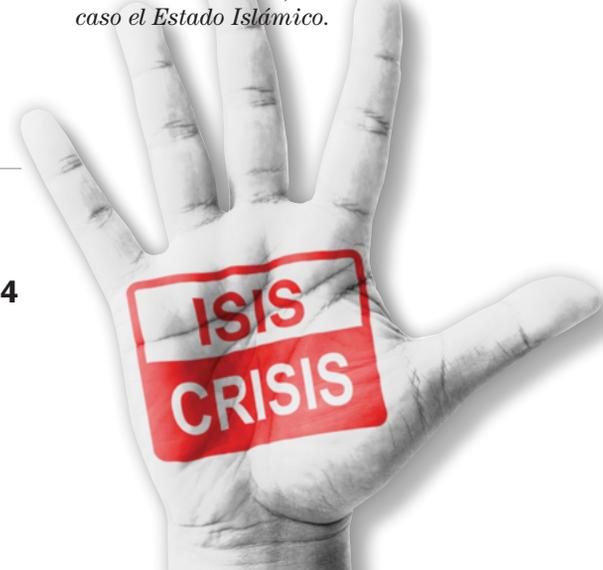
Aprenda sobre la historia y la evolución de esquemas BMPE y cómo las instituciones financieras son vulnerables a éstos.

Desechando el cuero para confeccionar una billetera electrónica 28

¿Está listo nuestro mundo tecnológicamente avanzado para tirar sus billeteras?

Evaluación del Estado Islámico y de grupos terroristas afines desde una perspectiva del ALD 40

Descubra la importancia de conocer a su cliente, o en este caso el Estado Islámico.





EN LA PORTADA

RECONOCIMIENTO **DE 2014** a la Clase

Presentación de los ganadores de los premios 2014 de ACAMS. . . . 32



52

TPPP: La delgada línea entre el riesgo y la eficacia 44

Incluir, o excluir TPPPs— esa es la cuestión.

La financiación del terrorismo: El atentado de Mumbai, un estudio de caso en lo posible y lo probable 46

Cómo el ataque terrorista de Mumbai de 2008 ayuda a dirigir nuestro futuro.

Consejos de FinCEN sobre una cultura de cumplimiento: Voz de alerta a la gestión de la institución financiera . . . 52

¿Cuáles son las funciones más importantes que las instituciones financieras, especialmente sus altos directivos, juegan mientras combaten el delito financiero?



56

La Cuarta Directiva de ALD/CFT de Europa 56

Los importantes cambios a la Directiva Europa de ALD ya que entra sus rondas finales de la consulta.

Orientación del Comité de Basilea sobre cómo gestionar el riesgo de LD y FT: Parte II, gestión a nivel de empresa y el papel de los supervisores en el ALD . . . 60

Cómo gestionar el riesgo del blanqueo de dinero en una organización por todo el grupo y fronteriza y el papel de supervisores.

La 13ª Conferencia Anual de ALD y Delito Financiero de ACAMS en un vistazo 64

Aquí está una vista exclusiva de la experiencia de la conferencia.



68

Delito fiscal y presentación de informes: ¿Una convergencia? 68

Herramientas sugeridas para los parámetros.

El evento inaugural del Capítulo de Greater Salt Lake City 72

El Capítulo de Greater Salt Lake City inició con 70 participantes de todo el valle de Salt Lake City.

Conozca al personal de ACAMS 74

Graduados de CAMS y de la Certificación Avanzada 75



Finales y comienzos nuevos

Felicitaciones Clase de 2014! Esta frase generalmente connota tiempo de graduación para la mayoría de nosotros. Graduarse generalmente significa el fin de un capítulo en nuestras vidas y el comienzo de uno nuevo. Las ceremonias de graduación son un momento para reconocer el trabajo y dedicación de los que se gradúan. Varios oradores imparten sabiduría, consejos y buenos deseos a los graduados. Tradicionalmente, estos oradores incluyen al graduado que da el discurso de despedida, el que da el de bienvenida y el orador invitado que ofrece el discurso de fondo. El orador invitado a menudo es alguien que tiene éxito en su campo de actuación.

A menudo, los discursos del mejor estudiante y el del que da el de bienvenida son los más memorables ya que son miembros de la clase que se graduó y estos discursos contienen experiencias compartidas de los años anteriores, las lecciones aprendidas y palabras de consejo. En esta entrega de *ACAMS Today*, tenemos un grupo de élite de premiados a los

que me gusta llamar la Clase de 2014. Estos ganadores tienen diversa formación con una amplia gama de experiencia en la industria de la prevención del delito financiero. Para mí, ellos son todos graduados de honor del campo de la prevención del delito financiero para 2014. Tuve el privilegio de entrevistarlos y aprender más sobre sus orígenes, experiencias, consejos y puntos de vista en sus carreras profesionales. Animo a los que lean estas líneas a aplicar los buenos consejos que dan nuestros premiados en el año por venir.

Esta entrega está llena de artículos interesantes sobre lo que los profesionales de ALD y prevención de delitos financieros se enfrentarán en el año 2015. El segundo artículo de portada, *Desechando el cuero para confeccionar una billetera electrónica* discute el futuro de la moneda y los desafíos que enfrentarán los profesionales de cumplimiento en la regulación del dinero virtual.

En el artículo *Diamantes: El mejor amigo del criminal*, el autor comparte una historia interesante de una señora mayor utilizada como

mula para transportar diamantes a través de las fronteras del país. Además, usted aprenderá acerca de las vulnerabilidades de los productos y comerciantes de metales preciosos, piedras preciosas y diamantes.

Lo que es más, usted podrá leer acerca de la Cuarta Directiva de ALD de Europa, los procesadores de pagos de terceros y la delgada línea entre el riesgo y la eficacia, la evaluación del Estado Islámico desde una perspectiva del ALD y mucho más.

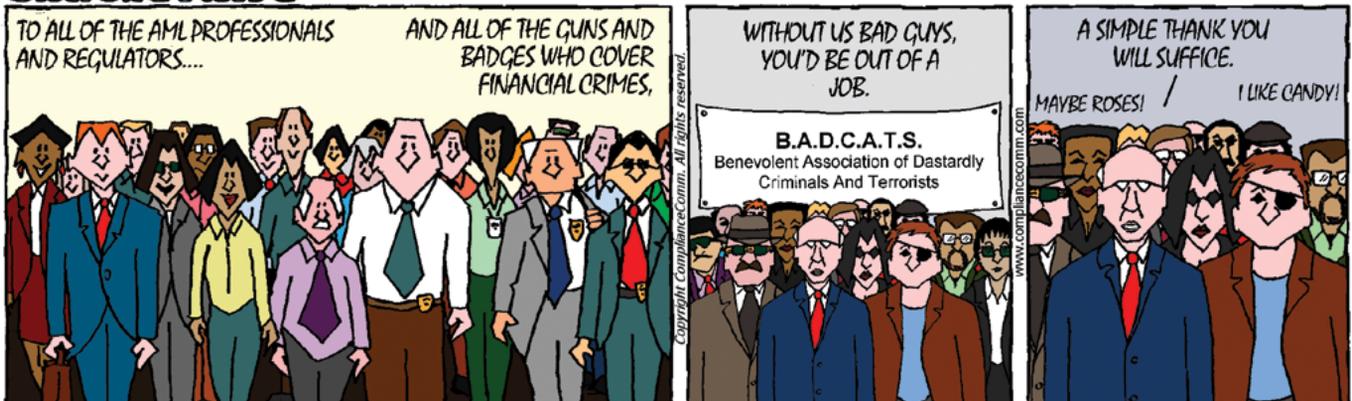
Una vez más, me gustaría felicitar a nuestros ganadores de los premios de ACAMS y sus muchas contribuciones a la industria.

Por último, a medida que 2014 llega a su fin y al comenzar un nuevo año, me gustaría animar a todos a continuar en el camino del aprendizaje y de fijar metas que ayudarán a lograr grandes cosas en 2015.

Me gustaría deseárselos a todos ¡Felices Fiestas y próspero Año Nuevo! **A**

Karla Monterrosa-Yancey, CAMS
jefa de redacción

SARSnSTRIPS™



Producido por ComplianceComm



LOOK BEFORE YOU REAP

Spotting opportunities in today's global markets is no easy task. Especially when there are dangers out there you never saw coming. Dow Jones Risk & Compliance is here to help. With an exclusive content set, market-leading tools and due diligence reports to help you assess and monitor high-risk situations. So you can seize the moment and the rewards.

dowjones.com/risk

**RISK &
COMPLIANCE**

Know What You're Getting Into.



Aaron Blankenstein, CAMS
Salt Lake City, UT, EE.UU.

Aaron Blankenstein ha sido oficial de GE Capital Bank (GECB) para la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) desde febrero de 2014. En este cargo, Blankenstein supervisa los esfuerzos para proteger a GECB de lavado de dinero y otras formas de ilícito en la actividad financiera. Tiene más de 14 años de experiencia en el sector bancario y ha trabajado en muchas áreas de cumplimiento de consumidores y cumplimiento comercial. Antes de entrar a GECB, sus funciones eran de construir y mantener el cumplimiento de BSA/ALD para Ally Bank, un banco comercial regulado por la FDIC y se centró en los servicios financieros automotrices y diversos productos de banca en línea (de los CD's, mercado de dinero, ahorros y cuentas corrientes). Blankenstein trabajó para Ally Bank por más de ocho años y fue nombrado oficial de BSA/ALD en 2011, donde se desempeñó hasta su marcha en febrero de 2014.

Blankenstein también sirve como representante y copresidente del recién creado capítulo de ACAMS de Greater Salt Lake City y está encantado de trabajar con estos profesionales de alta calidad en el área de Salt Lake.

Además, tiene un título de maestría en gestión organizacional y es Especialista Certificado en Antilavado de Dinero (CAMS).



Roy D'sa, CAMS
Columbus, OH, EE.UU.

Roy D'sa es vicepresidente senior y oficial mayor de la Ley de Secreto Bancario (BSA) en Huntington National Bank y tiene más de 30 años de experiencia en servicios financieros. Es un consumado profesional con experiencia bancaria significativa en las principales líneas de negocios, operaciones y funciones de apoyo. Ha ocupado puestos de liderazgo en la banca minorista, gestión de programas, banca electrónica, operaciones de consumo y comerciales, tecnología, fusiones e integración de adquisiciones y gestión de riesgos.

D'sa tiene experiencia de cumplimiento significativa en la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) y la Oficina de Control de Activos Extranjeros (OFAC) y lidera el programa de BSA/ALD de Huntington Bank para asegurar el cumplimiento de las leyes y reglamentos de BSA/ALD. Dirige un equipo de más de 90 miembros responsables de la gestión del riesgo del cliente y la debida diligencia, la evaluación del riesgo empresarial, inteligencia financiera, capacitación en BSA, cumplimiento de BSA/ALD y el cumplimiento de la OFAC.

D'sa está certificado con CAMS y es parte de la membresía empresarial de ACAMS. D'sa también participa en la Mesa Redonda de Bancos de tamaño mediano de la Oficina del Contralor de la Moneda (OCC), la Mesa Redonda de Servicios Financieros, los foros de BSA/ALD de Pares de Grupos de la Industria y conferencias de las agencias del orden público. Tiene un MBA en finanzas corporativas, y una Maestría en Ciencias y Licenciatura en ciencias de la computación.



Vicki Landon, CAMS-Audit
Austin, TX, EE.UU.

Vicki Landon es una profesional de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) que ofrece servicios de ALD y capacitación a instituciones financieras no bancarias. Formó Landon Associates hace cinco años para ayudar a las empresas a entender y manejar sus riesgos de ALD y fraude. Aprovecha décadas de experiencia en la entrega de soluciones de negocio para las instituciones financieras internacionales.

Landon se ha centrado exclusivamente en el ámbito del ALD durante los últimos 10 años. Ofrece auditorías independientes, evaluaciones de riesgos, formación y puesta a punto de los sistemas de monitoreo de transacciones, ayudando a las entidades no bancarias a asegurar que sus programas de cumplimiento sean eficaces y eficientes. Sus clientes van desde las aseguradoras designadas como instituciones financieras de importancia sistémica (SIFI) a las aseguradoras más pequeñas, agentes de bolsa y empresas de servicios monetarios (MSB).

Anteriormente, Landon fue vicepresidente de Aquilan Technologies, proporcionando soluciones de ALD a las aseguradoras. Ocupó cargos de liderazgo y ejecutivos en IBM y CSC, proporcionando orientación estratégica y táctica a las instituciones financieras.

Landon participa en elevar el nivel del profesionalismo de ALD con frecuencia a través de hablar en eventos del sector, seminarios por Internet y seminarios, y es cofundadora y copresidenta del capítulo de ACAMS del Centro de Texas. ACAMS publicó su libro blanco sobre la auditoría independiente de los sistemas de monitoreo de transacciones de ALD. Obtuvo la designación de CAMS-Audit con la clase inaugural y desde entonces ha sido miembro de la junta de revisión para las clases posteriores. Tiene nombramiento de Fellow, Life Management Institute (FLMI).



James Ninni
Chicago, IL, EE.UU.

James Ninni es un ex-nadador de búsqueda y rescate de la Armada de los Estados Unidos que realizaba rescates, recuperaciones y misiones humanitarias en España, Grecia, Italia, Francia, Túnez, Turquía, Israel, Cuba y Somalia. Ninni posee una licenciatura en finanzas y fue uno de los primeros en obtener una Maestría en administración de empresas de Ithaca College en 2001.

Poco después, Ninni se mudó a Chicago y comenzó a trabajar para una subsidiaria propiedad total de la Aon Corporation supervisando operaciones de cumplimiento, gestión de riesgos, seguridad y de préstamos de regulación en una cartera crediticia de \$4,3 mil millones.

En 2006, Ninni fue contratado como oficial de cumplimiento de mercados de capitales por la Federal Home Loan Bank de Chicago, una empresa bancaria patrocinada por el gobierno (GSE) de \$70 mil millones ofreciendo soluciones de préstamos al por mayor a instituciones financieras. Ninni ha supervisado a un alto nivel operaciones de banca e hipotecas que abarcan el cumplimiento normativo, la planificación estratégica, el desarrollo de negocios y la gestión de proyectos.

Ninni obtuvo un Certificado Sigma Seis, Certificado de Profesional de Tesoro (CTP), Certificado de Gerente de Resiliencia de Negocios (CBRM), y espera completar su Certificado de Especialista de Antilavado de Dinero (CAMS) a principios de 2015. Aprovechó esas habilidades para impulsar proyectos de mejora de toda la empresa y construir una sólida cultura de cumplimiento. Ninni construyó una reputación de mejora continua y minimización del riesgo a través de todas las actividades operativas.



Angeli Pereira, CAMS
Doha, Qatar

Angeli Pereira, especialista en antilavado de dinero/lucha contra el terrorismo financiero (ALD/CFT) con profunda experiencia regulatoria, es actualmente asociada senior en el dedicado equipo de ALD/CFT de la Autoridad Regulatoria del Centro Financiero de Qatar (QFC). En este cargo es responsable del ALD/CFT y de la vigilancia de delitos financieros de las instituciones financieras y actividades y profesiones no financieras designadas. Pereira supervisa las empresas respecto del cumplimiento de ALD/CFT para asegurar que las empresas adhieran a normas de ALD/CFT en el gobierno corporativo y comportamiento en el mercado, incluyendo las evaluaciones de riesgo principales y revisiones temáticas. Además, participa en iniciativas de ALD/CFT en todo el país, contribuye a mejorar el enfoque de supervisión y está involucrada en el proceso nacional de evaluación de riesgos.

Antes de unirse a la Autoridad Reguladora QFC, Pereira trabajó para la Unidad de Antilavado de Dinero y Casos Sospechosos (AMLSCU), la unidad de inteligencia financiera (UIF) en el Banco Central de los Emiratos Árabes Unidos, donde su papel incluía supervisar el cumplimiento a nivel nacional del ALD/CFT de las entidades que reportan, analizar informes de transacciones sospechosas y la recomendación de acción, lo que contribuye al ALD/CFT y la investigación de delitos financieros, el desarrollo de módulos de capacitación para sectores específicos y la realización de programas de capacitación y la identificación de tipologías predominantes en la región.

Como experta en la materia, Pereira es a menudo convocada para hablar en eventos y sesiones de capacitación y es una oradora muy conocida en la región. Ha sido miembro del Grupo de Trabajo MENA de ACAMS por dos años. Como representante, también ha participado en las sesiones plenarias, las reuniones del grupo y las sesiones de expertos del Grupo de Acción Financiera Internacional (GAFI), MENAFATF y otros organismos internacionales.

Además de su experiencia regulatoria, Pereira tiene experiencia en fusiones y adquisiciones, gobierno corporativo y funciones de secretaría de la empresa. Su experiencia profesional se apoya en los logros académicos, incluyendo un título del Instituto de Secretarios de Empresas de la India como secretaria de empresas, y licenciaturas en derecho (LLB) y comercio (B.Com). **FA**

Reading someone else's copy of

ACAMSTODAY?

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



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

ACAMS® Advancing Financial Crime Professionals Worldwide®

For more information and to join contact us by:

Phone +1 (866) 459-CAMS Outside U.S.: +1 (305) 373-0020

Fax: +1 (305) 373-7788 or +1 (305) 373-5229

Email: info@acams.org

Online: ACAMS.org ACAMSToday.org



La comprensión de los desafíos del ALD

Ya que el año 2014 llega a su fin, es el momento oportuno para hacer un balance de la comunidad del antilavado de dinero (ALD) y los temas que desafían nuestra membresía de ACAMS. Esta edición de *ACAMS Today* cubre muchas de estas áreas y da una idea de cómo estos temas están siendo abordados por profesionales de ALD.

La cultura de cumplimiento: Un concepto bien conocido por la comunidad de ACAMS

Kevin Anderson, *Al Gillum Volunteer of the Year* (el Voluntario Al Gillum de ACAMS) de 2014, cubre la reciente guía orientativa de la Red Contra los Delitos Financieros (FinCEN) del Departamento del Tesoro sobre la necesidad continua de una “cultura de cumplimiento”. Los profesionales de ALD siempre han creído en su misión y el desafío para todos nosotros es articular claramente por qué el apoyo de toda la empresa para cumplir—con todas las reglas y reglamentos cubiertos para ayudar a prevenir el movimiento de fondos ilícitos—son esenciales. Kevin ofrece una excelente hoja de ruta para el éxito.

Financiación del terrorismo—Nuestros intentos continuos de mantenernos actualizados

Hay una serie de artículos que profundizan en diversos aspectos de cumplimiento de ALD y el seguimiento de los fondos de los terroristas. Dennis Lormel ofrece ejemplos extraídos de las investigaciones del bombardeo de Mumbai en cuanto a cómo utilizar eficazmente la inteligencia financiera.

También tenemos un segundo artículo de Dennis que explica cómo abordar la actividad financiera del grupo terrorista del Estado Islámico (ISIS). Informes de prensa recientes han explicado cómo ISIS parece tener acceso al dinero de una manera diferente que grupos como al-Qaeda o Hamas. Dennis enfatiza el punto de “conocer al cliente” de una manera que no se ve con las estrategias anteriores de financiamiento del terrorismo. Usted puede estar seguro de que aquí en ACAMS vamos a seguir actualizando a los miembros en lo que hemos aprendido colectivamente con respecto a este grupo terrorista horrible que no respeta la vida humana.

La comprensión de los muchos temas que los profesionales de ALD necesitan saber

Cuando se creó *ACAMS Today*, la mayoría de los artículos cubrían las áreas tradicionales de cumplimiento: mantenimiento y presentación de informes sobre efectivo y cómo elaborar un informe de actividad sospechosa efectivo. En 2014, nuestros retos son mucho más extensos. Esta edición aborda la cuestión de cuánto más puede hacer la industria financiera para detectar, informar y prevenir la trata de personas. También tenemos en cuenta la evasión fiscal, la vulnerabilidad del lavado de dinero de los metales preciosos y una actualización sobre el cambio del peso en el mercado negro.

Como siempre, si tiene ideas para artículos, autores o entrevistas, por favor acérquese a nuestra jefa de redacción Karla Monterrosa-Yancey.

En memoriam

Uno de los momentos más tristes en una organización tan grande es cuando tenemos noticia de que alguno de nuestros socios ha fallecido. También es especialmente lamentable cuando perdemos un socio que era un tan firme defensor de la comunidad de ACAMS. En octubre, Shaun Hassett, un experto experimentado de OFAC/sanciones, nos dejó. Shaun trabajó en Thomson Financial durante 18 años y fue un pilar en la sala de exposiciones en las principales conferencias de prevención de lavado de dinero, así como en los paneles. Tenía un gran sentido del humor, era generoso con su tiempo con quien le pidiera ayuda y añadió tanto al área de cumplimiento de sanciones.

John J. Byrne, Esq., CAMS
vicepresidente ejecutivo

TODAY WE APPROACH RISK FROM EVERY ANGLE.

It's time you broadened
the scope of your
risk management
program with ERM.

Traditional approaches to risk management don't give you a complete picture of your risk. With CSI's SmartRisk IQ, you have access to an Enterprise Risk Management (ERM) solution that provides a real-time snapshot across all risk areas. Our platform changes your risk perspective through access to compliance tools and regulatory experts, making risk management more strategic and effective.

csiweb.com/seeitall



Diamantes:

El mejor amigo del criminal



Me encanta charlar con los funcionarios de aduanas, porque tienen las anécdotas más entretenidas. Han encontrado casi todas las maneras ingeniosas para tratar de pasar contrabando a través de una frontera. Aún así, un caso en febrero pasado en el Aeropuerto Internacional Pearson de Toronto debe haber levantado algunas cejas. El 3 de febrero, funcionarios de la Agencia de Servicios Fronterizos de Canadá (CBSA) detuvieron a una mujer de 66 años de edad tratando de entrar a Canadá desde Trinidad y Tobago. Como resultó, la anciana tenía 10.202 diamantes en bruto escondidos dentro de su cuerpo (o ‘envalijados’ en nuestra jerga cada vez más colorida de la aplicación de la ley). Alrededor de 1.500 quilates por valor de casi 400.000 dólares cayeron en cascada de su escondite.¹ El contrabando usando el cuerpo humano no es nada nuevo, pero la edad de la sospechosa y el número de piedras ocultas hacen de esta una historia convincente.

Los metales preciosos y piedras preciosas, en particular los diamantes, son un vehículo muy atractivo para ocultar y blanquear el producto del delito para financiar organizaciones terroristas y delictivas. Como los reguladores están cinchando las riendas sobre las instituciones financieras que hacen la colocación del producto del delito cada vez más difícil, podemos esperar que nuestros adversarios cambien sus estrategias y busquen otros medios para ocultar y convertir el dinero producto de la delincuencia. ¿Estamos, como investigadores, reguladores y entidades informantes prestando atención a los riesgos de lavado de dinero de los metales preciosos, piedras preciosas y diamantes? Voy a sugerir que no lo estamos, por lo menos no en mi país natal, Canadá.

Vulnerabilidades del producto

¿Qué pasa con los metales preciosos y las piedras preciosas que resultan tan atractivos para los lavadores de dinero y otros como

vehículo para convertir y ocultar el dinero producto de la delincuencia? El Grupo de Acción Financiera Internacional (GAFI) publicó un informe muy ilustrativo a principios de este año que examinaba riesgos del lavado de activos/financiamiento del terrorismo (LA/FT) en cada etapa de la cadena de diamantes.² El informe identificó una serie de características que hacen que los diamantes sean de alta vulnerabilidad como medio para el lavado de dinero de la delincuencia y el terrorismo financiero. La Tabla 1 resume algunas de las características más pertinentes.

Aunque el informe del GAFI se refería específicamente a los diamantes, otros tipos de piedras preciosas comparten estas mismas características.

Una de mis últimas tareas antes de retirarme de la actuación policial se logró mientras era detective en una unidad de vicio. Recuerdo una investigación particular que ilustra las observaciones del GAFI perfectamente. Detuvimos

a la persona que controlaba una empresa de prostitución interprovincial. Esta mujer tenía mucho éxito y manejaba su negocio de escoltas, así, como un negocio. Hicimos una orden de allanamiento en su oficina y obtuvimos cajas de registros de negocios, incluyendo los estados financieros anuales preparados por su contador. En el transcurso de unos pocos años, esta mujer generó una impactante cifra de \$9 millones en ingresos, gran parte de los cuales fueron ganancias producto del delito y que supo distribuir adecuadamente. Sus cuentas bancarias mostraron mucha actividad, pero sus balances eran todos muy bajos. ¿Qué hizo ella con sus ganancias del delito? Gastó un poco en un estilo de vida lujoso y algo invirtió en su propiedad residencial. Cuando abrimos la caja de seguridad en su banco nos alegramos de ver que estaba repleto de metales preciosos y piedras preciosas, incluyendo algunos relojes de alta gama. Algunas joyas eran claramente usadas, pero la mayoría eran piedras sueltas. El total estaba valorado de forma conservadora

¹ The Globe and Mail, “Woman Arrested at Toronto Airport Had 10,000 Diamonds Hidden in Body.” Ulicable en: <http://www.theglobeandmail.com/news-national/gems-seized-at-pearson-airport-destined-for-another-country-expert-suggests/article17032845/> Consultado el 16 de septiembre de 2014.

² Financial Action Task Force (FATF). “Money Laundering and Terrorist Financing Through Trade in Diamonds” October 2013. Consultado el 16 de septiembre de 2014 <http://www.fatf-gafi.org/topics/methodsandtrends/documents/ml-tf-through-trade-in-diamonds.html>

en más de \$100.000 y nos alegramos de apoderarnos del botín para el decomiso. El gerente del banco me dijo más tarde que se armó una escena cuando esta mujer llegó a la sucursal para recuperar su tesoro escondido y sólo encontró una caja de acero vacía. ¿Ha visto a un proxeneta tener un berrinche? ¡Es un espectáculo!

Vulnerabilidades comerciales

Como entidad que informa, los comerciantes de metales preciosos y piedras preciosas (DPMS según siglas en inglés) tienen al menos dos características que aumentan su susceptibilidad de ser utilizados en LA y FT: el tamaño de la organización y el alcance de su riesgo.

Tamaño de la organización: Hay aproximadamente 5.000 minoristas de alhajas en Canadá.³ Algunos son grandes cadenas nacionales o regionales, pero la mayoría son tiendas independientes, pequeñas, manejadas por sus dueños. La construcción y mantenimiento de un régimen de cumplimiento de ALD es mucho más difícil cuando la organización se compone de sólo dos o tres personas. Es difícil encontrar el tiempo o el desarrollo de los conocimientos técnicos necesarios para lograr y mantener el cumplimiento regulatorio.

Alcance del riesgo: A diferencia de muchas entidades informantes, un minorista DPMS debe considerar los riesgos tanto de transacciones de inventario como de venta al cliente. Los DPMS que compran alhajas de oro o de las personas ‘en la calle’ que quieren reciclar o simplemente convertir en efectivo sus alhajas tienen que mirar muy de cerca a estos proveedores y el origen de estos artículos de inventario. Incluso los DPMS minoristas que les compran a mayoristas DPMS de renombre deben tomar en cuenta el ALD/TF en su evaluación de los riesgos para ese proveedor.

Por lo tanto, teniendo en cuenta las características singulares de los diamantes (y otros metales preciosos y piedras preciosas), tipologías de LD/FT de los círculos policiales, así como las vulnerabilidades operacionales de los DPMS, a uno le gustaría pensar que los reguladores están en la parte superior de las cosas y la promoción del cumplimiento dentro de este sector. Productos altamente vulnerables al lavado de dinero y la financiación del terrorismo comprados y vendidos por comerciantes que, por la naturaleza de sus modelos

de negocio son altamente vulnerables, deben reconocerse como una gran bandera roja. Sin embargo, en Canadá al menos, este no parece ser el caso. Por lo menos todavía no.

En Canadá, el sector de DPMS se convirtió en una entidad que informa en 2008. Los minoristas y mayoristas de alhajas están obligados a tener el menú completo de herramientas de ALD y mecanismos de información en su sitio. Sin embargo, a pesar de estar sujetos a los requerimientos de la Ley y el Reglamento del Producto del delito (lavado de dinero) y Financiación del Terrorismo de Canadá durante seis años, el regulador del Centro

de las Transacciones Financieras y Análisis de Informes de Canadá (FINTRAC)⁴ da a los DPMS canadienses una calificación reprobatoria rotunda a la hora de cumplimiento.

A principios de este año presenté una solicitud de información a FINTRAC solicitando información sobre cuestiones de cumplimiento de los DPMS y los objetivos de organización de FINTRAC para este sector. Es comprensible que la salida de información estuviera fuertemente controlada y no se me dijo cuántos exámenes FINTRAC ha llevado a cabo en los DPMS. Sin embargo, alguna correspondencia interna que se publicó fue particularmente reveladora.

Tabla 1

Vulnerabilidades de productos de diamantes

-  Los diamantes tienen la capacidad de ganar, transferir y almacenar valor. Son un líquido y activo transferible.
-  La propiedad de un diamante puede ser transferida rápidamente, a menudo con poco o ningún rastro de auditoría.
-  A diferencia del dinero en efectivo, no se suele requerir informar de los diamantes que se transportan o cruzan las fronteras internacionales.
-  Los diamantes tienen un valor alto en relación con su tamaño, lo que los hace especialmente susceptibles de pasar como contrabando a través de fronteras internacionales.
-  El mercado de los diamantes es durable y disfruta de precios estables asegurando a los diamantes la capacidad de retener y adquirir valor con el tiempo.
-  Una vez que los diamantes entran en el mercado lícito son difíciles de rastrear en términos de propiedad y origen.
-  Los diamantes son fácilmente comprados y vendidos fuera del sistema bancario formal evitando así salvaguardias robustos de antilavado de dinero (ALD) y conozca a su cliente (KYC).
-  La evaluación del precio de los diamantes es altamente calificado y por lo tanto vulnerable a la manipulación para ocultar su verdadero valor de mercado.
-  Los diamantes, como el oro y la plata, se pueden utilizar como moneda.

³ Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Acceso a la Información solicitado por el autor el 31 de julio de 2014.

⁴ Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Consultado el 16 de septiembre de 2014 <http://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp>

En ella, un oficial de FINTRAC hizo una serie de observaciones sobre cumplimiento de los DPMS en los ámbitos de la política y procedimientos, evaluación de riesgos, la formación continua y el cumplimiento de la revisión del programa de dos años. Aquí registro un poco de lo que el funcionario dijo:

“La mayoría de los regímenes de entrenamiento de cumplimiento existentes que fueron revisados durante el curso de un examen eran completamente deficientes”.

“La mayoría de las entidades informantes [RE] recibió deficiencias totales por revisiones [de dos años], incluso si tenían otros elementos del régimen en su lugar”.

Esta evaluación se prolonga por dos páginas y pinta un panorama sombrío a través de casi todos los elementos del régimen de cumplimiento de los DPMS. Realmente no hay puntos brillantes. Esta autor interno privilegiado de FINTRAC también comentó que los equipos de cumplimiento tipo ‘hágalo usted mismo’ de los DPMS, si bien eran potencialmente un buen punto de partida para un DPMS, son mecanismos inadecuados y poco fiables para construir un régimen de ALD que cumpla con los requisitos legales de Canadá. Un régimen de cumplimiento, especialmente la evaluación de riesgos y los requisitos de la política y de procedimiento, debe personalizarse para las operaciones de negocio y riesgos de cada joyero individual. Los productos estandarizados simplemente no cumplen en este sentido. Los joyeros—especialmente las pequeñas empresas—en realidad sólo tienen dos opciones para asegurar el cumplimiento: invertir y desarrollar la experiencia interna o depender de un consultor calificado.

Más allá de errar el blanco para su propio sector, los joyeros morosos y que incumplen también causan un riesgo operacional para las instituciones financieras que tienen cuentas de DPMS. Teniendo en cuenta los requisitos reglamentarios de ALD/ FT para los DPMS y las instituciones financieras, las vulnerabilidades de metales preciosos y piedras preciosas, y la naturaleza global de la industria de la joyería, las instituciones financieras deberían prestar especial atención a sus clientes DPMS. Como

parte de su programa de diligencia debida del cliente (DDC), las instituciones financieras pueden querer insistir en que los titulares de cuentas de DPMS demuestren que cumplen con sus obligaciones legales de ALD/FT. ¿Puede el joyero proporcionar una copia de la evaluación basada en el riesgo de la empresa, el manual de capacitación de ALD/FT, o la revisión independiente? ¿Ha sido examinado alguna vez el DPMS por el regulador? Si es así, ¿cuáles fueron los resultados? ¿Qué tipo de transacciones financieras ejecuta el DPMS, en qué jurisdicciones, y con quién? La institución financiera realmente tiene que mirar de cerca las actividades de negocio DPMS.

Así que, ¿qué podemos esperar del regulador de Canadá cuando se trata de los DPMS? Algunos factores apuntan a un mayor escrutinio en el horizonte. Hasta el momento, FINTRAC todavía tiene que evaluar una sanción pecuniaria administrativa (AMP) a un DPMS a pesar del pobre historial de cumplimiento por parte del sector.⁵ Canadá no lo hizo tan bien en nuestro primer informe de evaluación mutua (MER) del GAFI en 2008, pero mejoramos y logró el cumplimiento del GAFI en nuestra evaluación de seguimiento de 2014. Espere usted que el reciente informe del GAFI sobre las vulnerabilidades del ALD/FT de la cadena de diamantes sea examinado minuciosamente por FINTRAC. Somos un Estado del G-7 y uno de los miembros fundadores del GAFI. Considere usted también que para el valor, Canadá es el tercer mayor productor y exportador de diamantes en el mundo y que incluso están empezando a cortar y pulir nuestros diamantes aquí.⁶ Todo esto es para decir que Canadá se preocupa mucho acerca de las evaluaciones del GAFI y quiere proteger y promover la industria de los diamantes canadienses.

Teniendo en cuenta los muy bajos niveles de cumplimiento de DPMS, la falta de aplicación significativa, y el punto de mira del GAFI iluminando las vulnerabilidades de los diamantes de LA/FT, quiero anticipar que FINTRAC intensificará su vigilancia del cumplimiento de DPMS en un futuro próximo y mejorará este sector por un par de puntos en nuestra evaluación nacional de riesgos.

El cumplimiento de ALD tiene que ser un tema permanente del programa para los propietarios de la empresa y la junta directiva



Para los oficiales de cumplimiento de DPMS esto significa que su evaluación de riesgos, las políticas y procedimientos, capacitación continua y revisiones independientes deben ser una prioridad de la organización. Consulte usted la página Web de su unidad de inteligencia financiera (UIF), estudie la legislación, lea las directrices de interpretación, investigue las sanciones emitidas a otras entidades informantes, y si es necesario, obtenga usted asistencia calificada. El cumplimiento de ALD tiene que ser un tema permanente del programa para los propietarios de la empresa y la junta directiva. Comparta usted con la alta dirección y que sea consciente de sus obligaciones legales en este sentido. Tenga usted una evaluación severa de su régimen de cumplimiento y pregúntese si usted está preparado para un escrutinio mayor. **AI**

Ken Brander, CAMS, CFE, MDY, detective retirado del Servicio de Policía de Edmonton y fundador de Clarium Fraud and Compliance Solutions Ltd., Alberta, Canadá, kenbrander@telus.net

⁵ Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Consultado el 16 de septiembre de 2014 <http://www.fintrac-canafe.gc.ca/pen/4-eng.asp>

⁶ Financial Action Task Force (FATF). “Money Laundering and Terrorist Financing through Trade in Diamonds” October 2013, p. 31. Consultado el 16 de septiembre de 2014 <http://www.fatf-gafi.org/topics/methodsandtrends/documents/ml-tf-through-trade-in-diamonds.html>



Industrial Strength Offerings for **Sanctions & PEP Screening, KYC / CIP and Identity Verification**

**Handles Unlimited
Record Volumes**

100% SaaS Up-time

**Verified Disaster
Recovery Plan**



*Available as licensed or
hosted (including interactive
web services calls), desktop,
and appliance*



*16 billion+ hosted
transactions per year*

Built upon Innovative Systems, Inc.'s (ISI) 45 years of data matching expertise, FinScan's "intelligent" linking technology **minimizes:**

- ✓ **the risk of missing real matches (false negatives)**
- ✓ **the volume of false matches (false positives)**
- ✓ **the time and cost required to research potential matches.**

- Integrates smoothly with all leading third-party PEP databases
- Helps ensure the accuracy and validity of SWIFT and other payment transaction processing
- Provides sanctions lists and 24/7/365 list management service
- Integrates with selected scanners to import information from driver's licenses, passports, and other forms of government I.D.
- Automates review process through an integrated case management tool
- Facilitates customer onboarding
- Screens available in English, Spanish, French, German, and more
- Plus many other features, including document attachment

www.finscan.com



Global Headquarters - USA
+1.412.937.9300 x8237
info@innovativesystems.com

EMEA Headquarters - London
+44 (0) 20 7422 6310
infouk@innovativesystems.com

PITTSBURGH • TORONTO • MEXICO CITY • LONDON • FRANKFURT

Dos componentes cruciales en la LUCHA CONTRA LA TRATA DE PERSONAS

Mientras observaba la repetición del primer foro sobre *La Lucha Contra la Trata de Personas*, celebrada el 9 de abril del 2013 en la Casa Blanca, no solo me sorprendía por la postura y la pasión de este tema, sino también por los recursos que se están estableciendo y las medidas adoptadas a nivel federal para cumplir con ello. Aunque me sentí empoderado y asombrado ante estos esfuerzos, también me sentí derrotado y confundido al mismo tiempo.

El foro contó con muchos funcionarios de la Casa Blanca que resaltaron y explicaron los cuatro compromisos que se están tomando en este esfuerzo, expuestos por el Presidente Barack Obama en su discurso de la Iniciativa Global Clinton en 2013. Si bien estas cuatro iniciativas implican elementos amplios, las ideas principales incluyen: primero, la prevención de la trata de personas por medio de la concientización de las poblaciones vulnerables; segundo, la educación del público y de los respondedores públicos; tercero, el enjuiciamiento mediante el fortalecimiento de las investigaciones y las medidas coercitivas; y cuarto, la protección de la sociedad y la prestación de apoyo a las víctimas por medio de los servicios sociales.

Mientras escuchaba todos estos asombrosos esfuerzos, y el énfasis sobre las fuerzas del orden, servicios de apoyo, etcétera, pensé, “¿Dónde encajo yo como profesional financiero?” “¿Cuál es el tema común en la trata de personas (HT según sus siglas en inglés)?” “¿Cuál es la fuerza impulsora detrás de ella?” La respuesta es el dinero. ¿Quién mejor para combatir la HT que los de las instituciones en las cuales estos fondos podrían fluir a través de?

Al reflexionar sobre toda esta información, volví a las conversaciones tenidas con otros sobre este tema y también me hizo pensar en las empresas de las que he sido parte y qué medidas tomaron en esta lucha. Inmediatamente, me acordé de una conversación en la que abordamos este tema y en la que se hizo una referencia inicial de la película *Taken*, protagonizada por Liam Neeson, en la que hubo un secuestro con fines de esclavitud sexual de la hija de un ex agente de la CIA por traficantes de personas. Muchos compañeros hicieron comentarios que demostraron que a sus ojos no sólo la HT es solamente acerca de la esclavitud sexual, sino que sólo se produce en lugares “extranjeros”. Esto, a su vez, me contó una historia de una completa falta de educación sobre esta cruel realidad. Pensé más acerca de las distintas empresas de las que he sido parte y lo que he aprendido acerca de este tema mientras estaba allí. Rápidamente me di cuenta de que todo lo que había aprendido en torno a este tema había sido autodidactismo a través de la información en línea y los recursos proporcionados por ACAMS, la Red Contra los Delitos Financieros (FinCEN) y el FBI; que nunca había recibido ningún tipo de formación real sobre el tema, y estaba completamente ajeno a las medidas adoptadas por las empresas de que yo había sido parte. ¿Cómo fue posible esto? ¿Cómo es que los profesionales financieros, que están en algunas de las mejores, si no la mejor posición para hacer una diferencia y poner fin a esta lucha no están entrenados a fondo sobre este tema? ¿Y cómo es que la idea de que a los profesionales financieros no se les considera prioritariamente una baza en esta lucha desde una perspectiva federal?

Mientras tomo lo que sé sobre el tema, rápidamente me di cuenta de que como profesionales financieros estamos en una buena posición y también estamos en una de las posiciones más difíciles de detectar que no hay banderas rojas de HT absolutas, sino más bien banderas rojas que pueden hacerse pasar por otra actividad delictiva, y/o como otra actividad legítima. Pensando en varios ejemplos, elijo una bandera roja: la renuencia o negativa de los individuos a proporcionarle información de identificación a un bancario. Esto podría indicar HT, contrabando de drogas, un esquema de fraude o incluso nada ilegal en absoluto. Lo mismo con la actividad estructurante, un cambio repentino inexplicable en la actividad bancaria, o una falta de correspondencia entre las cantidades pagadas y la ocupación de la persona— los ejemplos podrían seguir y seguir.

Ante estos desafíos, dos cosas muy específicas deben ocurrir dentro de las instituciones financieras para ayudar a apoyar esta causa. Primero y principal es la educación del personal. Al

igual que se le requiere a una firma financiera llevar a cabo formación anual obligatoria en antilavado de dinero (ALD) o de la Oficina de Control de Activos Extranjeros (OFAC), la formación en HT debe aplicarse y debe cubrir no sólo lo que es la HT y el hecho de que puede suceder y de hecho sucede cerca, sino también la gravedad del tema y las banderas rojas con las que podrían asociarse. Y si bien se observa que no hay banderas rojas directas, el tema principal en los ejemplos mencionados anteriormente es que la actividad es de hecho inusual y necesita primero ser reconocida y después informada por empleados de las instituciones financieras. Esto establecerá una base sólida de personal entrenado y, a su vez, haría reconocer al personal estas señales de alerta, lograr que haga las preguntas correctas e informar a las personas que correspondan.

En segundo lugar, pero tan importante como lo primero, es el amplificador de monitoreo de transacciones dentro de las instituciones financieras. Las orientaciones dadas en torno a algunos de los posibles indicadores financieros de HT comunes se centran en cosas como la transferencia de fondos sin relación lógica con el remitente de los fondos, o el uso frecuente/inusual de depósitos nocturnos o cajeros automáticos para depósitos, junto con muchos otros; la mayoría de los cuales sólo pueden ser detectados a nivel transaccional. Teniendo en cuenta el ejemplo de uso frecuente e inusual de depósitos nocturnos o cajeros automáticos, un sistema de monitoreo transaccional típico puede revisar estos tipos de depósitos y alertas, generará su revisión sobre la base de la superación del umbral de la frecuencia dada de transacciones y/o la cantidad total dentro de un marco de tiempo especificado. Esto puede o no dar lugar a una alerta de sospechas para depósitos nocturnos inusuales dependiendo de esos umbrales.

Dado este escenario, conviene fijar umbrales aún más diversificados, teniendo en cuenta factores adicionales como depósitos nocturnos entre las 10 de la noche y las 6 de la mañana, o los que se producen en diferentes cajeros automáticos alrededor de la ciudad o incluso en diferentes estados. Tomando este mismo ejemplo, considérese lo siguiente: Durante el plazo de un mes, una cuenta muestra 30 depósitos de cajeros automáticos por \$100 cada uno, otra cuenta muestra 30 depósitos de cajeros automáticos por \$100 cada uno, todos los cuales ocurren entre la 1 y las 3 de la mañana en los cajeros automáticos en cinco estados diferentes a través de los EE.UU.

La realidad es que la actividad anterior es para la misma cuenta, pero la historia que cuenta es una completamente diferente una vez que consideremos factores adicionales. El monitoreo de transacciones se debe hacer de la misma manera. Añadir umbrales y personalizar y comprobar constantemente puede realmente hacer una diferencia, no sólo en la detección de una posible actividad de HT, sino de la actividad sospechosa en general. Además, las alertas que generan, a su vez, serán mucho más valiosas y reducirán la cantidad de falsos positivos que resultan en esfuerzos inútiles. A pesar de que sería casi imposible decir que cierta actividad transaccional es una prueba absoluta de la actividad de HT, la personalización y la adición de mayor diversidad a la vigilancia ayudará a asegurar alertas valiosas, y, a su vez, hará investigar esa actividad, y escalarla a las autoridades adecuadas.

Primero y principal es la educación del personal

Mientras, tanto el entrenamiento como la capacitación de los empleados y la mejora de la supervisión de las transacciones parece bastante elemental, son componentes cruciales en este combate. Los insto a todos a pensar en lo que se está haciendo dentro de sus propias empresas y lo que pueden hacer para ayudar en esta lucha que se está recuperando a nivel federal. Por favor haga usted su parte en la investigación dentro de su propia institución financiera sobre qué recursos hay. ¿Existe formación centrada en la HT, y su monitoreo de transacciones detecta adecuadamente la posible actividad de HT? Si no, haga un punto para traer este tema a la vanguardia en estas áreas; póngase en contacto con los actores clave dentro de estos grupos y vea cómo se puede ayudar en este esfuerzo. Aunque los profesionales financieros no fuimos convocados específicamente, somos un activo fundamental en esta iniciativa global para finalizar la HT. 

Brandy Wagner, CAMS, supervisión y gestión de ALD, Chicago, IL, EE.UU.

LAS EMPRESAS DE SERVICIOS MONETARIOS

¿Víctimas del enfoque basado en el riesgo?

Impulsados por los recientes casos de alto perfil, tales como la multa de 1,9 mil millones de dólares por lavado de dinero de HSBC, los bancos han estado echando un buen vistazo a su perfil de riesgo. Esto ha dado lugar a que muchos bancos finalicen los servicios bancarios para las empresas de servicios monetarios (MSB según siglas en inglés). Barclays, por ejemplo, tomó la decisión en 2013 de cerrar alrededor de 250 cuentas de MSB,¹ lo que ha tenido un gran impacto en las comunidades de expatriados locales y la economía de los países en desarrollo, tales como Somalia.²

No hay que olvidar que la lucha contra el lavado de dinero y la financiación del terrorismo es una tarea importante y difícil. En 2011, la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD) estimó que 1,6 mil millones de dólares, o 2,7 por ciento del PIB mundial fue lavado por delincuentes. Los bancos y las MSB tienen un papel importante que desempeñar en esta lucha contra la delincuencia, pero si se cierra cuentas de MSB es esto realmente una solución a la lucha contra la delincuencia o es que solo está alimentando el fuego?

¹ <http://www.theguardian.com/global-development/2013/sep/30/somalia-remittances-barclays-bank-dahabshiil>

² <http://www.atlanticcouncil.org/publications/external/intelbrief-barclays-and-the-somali-remittances-crisis>

La importancia de las MSB

Los principales bancos internacionales no tienen el deseo de ofrecer servicios de remesas a un gran número de clientes de poco valor. Por lo tanto, las MSB desempeñan un papel vital en la prestación de servicios de remesas a la comunidad y a los “no bancarizados” expatriados. Al eliminar este canal de financiación, estos “no bancarizados” y expatriados se verán obligados a utilizar los canales más caros, poco fiables e informales. El dinero va a llegar a meterse en maletas, pasar como contrabando a través de fronteras y es más probable que termine en las manos de delincuentes y extremistas.

Según el World Bank, se estima que, en todo el mundo, los flujos de remesas alcanzaron \$550 mil millones en 2013 y pueden llegar a más de \$700 mil millones para el 2016.⁴ Las remesas son ahora casi tres veces el monto de la ayuda oficial para el desarrollo y mayor aún que la deuda privada y la cartera de renta variable que fluye a los países en desarrollo. Superan las reservas de divisas en al menos 14 países en desarrollo, y son equivalentes a por lo menos la mitad del nivel de las reservas en más de 26 países en desarrollo. A medida que los mercados emergentes se enfrentan a un debilitamiento de la balanza de pagos, la importancia de las remesas como una fuente de ingresos en divisas es cada vez mayor.

Enfoque basado en el riesgo frente al basado en reglas

Las 40 Recomendaciones revisadas del GAFI emitidas en 2012 se centraron más en la adopción de un enfoque basado en el riesgo.

Los bancos aprovecharon esta oportunidad para revisar sus evaluaciones de riesgo del cliente.⁵ Con muchas reglamentarias frescas en sus mentes, los bancos tenían menos apetito para servir a los clientes de alto riesgo. Como resultado, muchas MSB legítimas, bien administradas, se convirtieron en víctimas del enfoque basado en el riesgo.

En lugar de la gestión de los riesgos, los bancos comenzaron a salir del mercado de MSB completamente. Esto envió una señal a otros bancos que había algo malo con todas las MSB y como resultado de un efecto dominó de cierres de cuentas está sucediendo en todos los ámbitos.

Por lo tanto, ¿las multas reglamentarias y la aplicación del enfoque basado en el riesgo tienen el efecto deseado? ¿Se está atrapando a más los lavadores de dinero o simplemente se ha dado lugar a que muchos clientes inocentes sean víctimas?

Tal vez el mercado no está lo suficientemente maduro para un enfoque basado en el riesgo y sin la reglas de apoyo. Hay directrices emitidas por el Grupo de Acción Financiera Internacional (GAFI) y los reguladores, pero tal vez no van lo suficientemente lejos para que los bancos se sientan seguros de que están gestionando sus riesgos lo suficiente como para evitar multas reglamentarias.

Tómese el caso del HSBC, por ejemplo, la multa no era por el blanqueo de capitales o de las cuentas de haberes de MSB sino porque tenían controles internos débiles. Con la ausencia de reglas claras, la reacción de muchos de los bancos internacionales ha sido cerrar cuentas de MSB, lo que implica que son de riesgo demasiado para tratar con ellas.

¿Qué pueden hacer los organismos internacionales?

- Una certificación reconocida a nivel internacional, similar a una “norma ISO” de un organismo internacional establecido podría ayudar a las MSB a que desarrollen un programa de cumplimiento fuerte y que las puedan demostrar como tal. Este “sello de aprobación” daría a los bancos una mayor comodidad para mantener cuentas de MSB con programas de cumplimiento certificados.
- Invitar a los representantes de MSB a hablar en conferencias y demostrar cómo funcionan sus programas de cumplimiento. Esto ayuda a elevar el perfil de las MSB y educa a los oficiales de cumplimiento de los bancos, por lo que sienten más cómodo el manejo de estas cuentas.

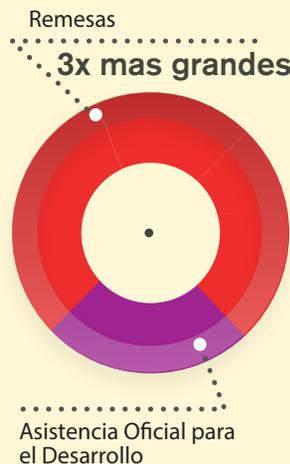
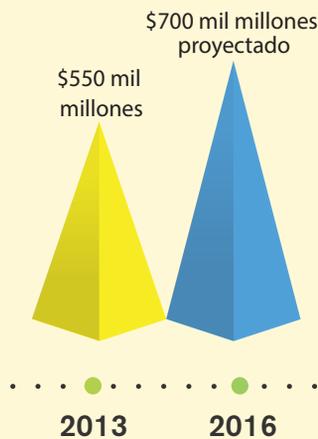
¿Qué pueden hacer los reguladores?

Los bancos corresponsales son menos propensos a mantener cuentas de MSB en jurisdicciones mal reguladas. Los reguladores deben hacer cumplir los reglamentos coherentes en todas las MSB bajo su control. Muchos países tienen regulaciones de MSB que cumplen con las Recomendaciones del GAFI. Sin embargo, en realidad, no están siendo seguidos de manera uniforme por todas las MSB.

Los clientes siempre van a ir a la MSB más barata, más conveniente. Conveniencia significa que no se hagan preguntas o tenga que llenar formularios y proporcionar justificantes de las transacciones.

Las MSB que están tratando de seguir las regulaciones del antilavado de dinero estrictamente suelen ser penalizadas con la pérdida de negocio, que va a las MSB más laxas.

Flujos de Remesas



³ <http://www.UNODC.org>: Illicit money: how much is out there? 25 October 2011

⁴ Migration and Remittance Flows: Recent Trends and Outlook, 2013-2016, 2 October 2013, The World Bank

⁵ <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html>

Los reguladores tienen que ser más proactivos en el apoyo a la banca de las MSB. Establecer directrices claras sobre los requisitos de diligencia debida de MSB, por lo que los bancos se sienten más seguros de que están manejando sus cuentas correctamente y no están en riesgo de multas regulatorias a las MSB bancarias.

Eso no quiere decir que los esfuerzos no están ya desplegados por los reguladores. Por ejemplo:

- En abril de 2014, la Autoridad de Conducta Financiera (FCA) advirtió una vez más a las empresas que no espera que bajen los clientes innecesariamente simplemente para evitar el riesgo de lavado de dinero. Tracey McDermott, directora de la FCA en la aplicación y la delincuencia financiera, dijo que el regulador “rara vez esperaría que las empresas salgan de relaciones de negocios por evitar riesgos”. Ella dijo “es poco probable que sea la única solución para el problema. No queremos terminar teniendo un mundo donde el miedo a las consecuencias... les negará a las personas el acceso a los servicios legítimos”.⁶

Es esencial que las organizaciones bancarias ni definan ni traten a todas las empresas de servicios monetarios como si presentaran el mismo nivel de riesgo

- A principios de 2014, el Grupo Mixto de Dinero Lavado de Dirección (JMLSG por siglas en inglés) publicó para el comentario una propuesta de Orientación sobre MSB (como clientes de los bancos).⁷
- En 2005, la FinCEN emitió directrices para las MSB bancarias.⁸ En este documento se establece lo siguiente:

“Al igual que con cualquier categoría de titular de cuenta, habrá negocios de servicios monetarios que representan poco riesgo de lavado de dinero y los que plantean un riesgo significativo. Es esencial que las organizaciones bancarias ni definan ni traten a todas las empresas de servicios monetarios como si presentaran el mismo nivel de riesgo... Si la evaluación de riesgos de una entidad bancaria indica potencial de un mayor riesgo de

blanqueo de capitales o financiación del terrorismo, se espera que lleve a cabo la debida diligencia de manera acorde con el aumento del riesgo. Esto no es diferente de los requisitos aplicables a cualquier otro cliente de negocios y no significa que una entidad bancaria no puede mantener la cuenta”.

Los reguladores podrían también:

- Dar a conocer las medidas de aplicación adoptadas contra las MSB en caso de incumplimiento de regulaciones sobre el ALD. Si no se hace público, la MSB será complaciente y no tomará en serio las regulaciones pensando que no hay consecuencias.
- Insistir en las normas mínimas de formación para los responsables de cumplimiento de una MSB. Un título reconocido como Especialista Certificado en Antilavado de Dinero (CAMS en inglés) o de la finalización de otros cursos reconocidos por el regulador debería ser obligatorio antes de que un regulador apruebe el nombramiento de una posición de cumplimiento.
- Establecer procedimientos acordados por los auditores para auditar el cumplimiento de las MSB. La calidad de las auditorías de cumplimiento de ALD varía ampliamente entre los diferentes países. Un banco corresponsal tendrá mucha más comodidad de recibir una auditoría transparente detallada que demuestra que ha cubierto todas las áreas del cumplimiento de las MSB en lugar de unas pocas líneas que indican que la MSB es compatible con todos los requisitos reglamentarios.
- Poner en práctica central el monitoreo de transacciones de MSB. Las transacciones por encima de cierto valor podrían ser subidas a los reguladores de base de datos central sobre una base diaria o mensual y examinadas con los sistemas automatizados de control. Si las MSB saben que están siendo vigiladas son mucho más propensas a cumplir con los reglamentos y llevar a cabo la debida diligencia en sus clientes.

¿Qué pueden hacer los bancos?

La banca de MSB tiene sus ventajas. Las cuentas de MSB tienen un alto volumen de transacciones y por lo tanto son buenos productores de los ingresos por comisiones. En el entorno actual, los clientes de MSB son muy leales a sus relaciones bancarias existentes. Una MSB bien dirigida también hace buenos clientes de crédito. Los bancos que pueden llegar a estar familiarizados con los riesgos que rodean estas cuentas y aprenden a gestionarlos adecuadamente, a menudo encuentran que tienen relaciones bancarias sólidas y rentables.⁹

FinCEN da directrices claras sobre cómo llevar a cabo una diligencia debida (EDD) en MSB:

- Revisar el programa de ALD de la MSB
- Revisar los resultados de pruebas independientes de la MSB de su programa de ALD
- Llevar a cabo visitas sobre el terreno

⁶ FCA warns firms again about AML ‘de-risking,’ Compliance Complete, Martin Coyle, April 30, 2014

⁷ <http://www.jmlsg.org.uk/news/guidance-on-money-service-businesses-as-customers-of-banks>

⁸ Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses operating in the United States http://www.fincen.gov/statutes_regs/guidance/pdf/guidance04262005.pdf

⁹ 6 Steps for Community Banks to Succeed with Money Services Businesses, ABA Bank Compliance, January/February 2006, Kathlyn L. Farrell

Los Flujos de Remesas superan



reservas en divisas en al menos 14 países en desarrollo

equivalente a la



mitad del nivel de reservas en más de 26 países en desarrollo

- Revisar la lista de agentes, incluyendo lugares, dentro o fuera de los EE.UU., que va a recibir los servicios directamente o indirectamente a través de la cuenta de MSB
- Revisar los procedimientos por escrito para el funcionamiento de la MSB
- Revisar las prácticas escritas de gestión y de terminación de agente para la MSB
- Revisar las prácticas escritas de cribado de empleados para la MSB

La EDD incurre en costos adicionales para los bancos; sin embargo, hay precedentes para tomar este costo en cuenta al formular la fijación de precios para las cuentas de MSB. Los bancos podrían cobrar una tarifa plana para todos los clientes de MSB con cargos adicionales en función de la actividad de la cuenta.

Bancarizar a las MSB y trabajar con ellas para mejorar su programa de cumplimiento debe considerarse buena responsabilidad social corporativa. No sólo se está ayudando a la sociedad en su conjunto, sino que también se está ayudando a la comunidad local ayudándola a enviar dinero a sus seres queridos.

¿Qué pueden hacer las MSB?

Sólo se necesita una MSB con controles internos débiles para dañar la reputación de todos las demás. Las MSB deben trabajar juntas para mejorar la fuerza de sus programas de cumplimiento en toda la industria. Establecer asociaciones locales de MSB para compartir retos e ideas. Invitar a los reguladores y unidades de inteligencia financiera (FIU) para asistir a las reuniones y dar orientación sobre áreas de cumplimiento que deben mejorar y actualizar sobre las tendencias del lavado de dinero y sus tipologías.

La alta dirección de las MSB necesita demostrar seriedad en el cumplimiento y respeto de sus obligaciones reglamentarias. Puede hacerlo mediante la contratación de profesionales de cumplimiento debidamente capacitados para ejecutar su programa de cumplimiento. Todavía es común ver que a un miembro joven del personal se le da la responsabilidad de cumplimiento y luego ningún apoyo para desarrollar sus conocimientos o implementar los controles necesarios.

Conclusión

Con el cierre de las cuentas bancarias, las MSB se ven obligadas a superar su juego. Las MSB con un programa de cumplimiento fuerte estarán dispuestas a cumplir con ello, pero necesitan el apoyo de los bancos, los reguladores, los gobiernos y los organismos internacionales.

Tenemos que hacer que las MSB constituyan una industria de renombre, altamente regulada con el fin de apoyar la estabilidad financiera y garantizar que el flujo de efectivo a través de las fronteras no sea impulsado a las manos de delincuentes y extremistas. **FA**

Rosanna Deamer, MSc, CAMS, MICA, CFE, jefa de cumplimiento, Bahrain Financing Company, Manama, Bahrain, rosannadeamer6@hotmail.com

Las opiniones expresadas en este artículo son las de su autor y no representan necesariamente la opinión de Bahrain Financing Company.

La trama del Mercado Negro de Cambio de Pesos:

El pasado, el presente y el futuro probable



El 10 de septiembre del 2014 la redada federal de cerca de 70 localidades en el distrito de la moda de Los Ángeles que condujo a la histórica incautación de \$100 millones en efectivo, nueve detenciones y el inicio de las investigaciones a largo plazo contra varias corporaciones por parte del Departamento de Justicia (DOJ) de los EE.UU. pusieron en primer plano, una vez más, la trama del lavado de dinero conocida como el Mercado Negro de Cambio de Pesos (BMPE, por sus siglas en inglés).

No es la primera vez que la trama de BMPE fue traída a la atención del público e investigadores federales estadounidenses. De hecho, en 1997 la Red Contra los Delitos Financieros (FinCEN) emitió advertencias relativas a los regímenes de BMPE y advirtió de banderas rojas. El 21 de junio del 1999, se proporcionó amplio testimonio ante el congreso sobre el esquema de BMPE colombiano y se observó que el tráfico de drogas genera más de \$55 mil millones por año y que aproximadamente \$5 mil millones se lavan al año. Además, antes de la redada del 10 de septiembre del 2014, el DOJ obtuvo órdenes de aprehensión en contra de tiendas de juguetes lujosas que participaron en las tramas del BMPE y se cree que colectivamente lavaron más de \$14 millones durante el período de tiempo considerado.

Así que, ¿por qué deberían los profesionales de cumplimiento antilavado de dinero (ALD) preocuparse por la trama de BMPE?

1. La trama de BMPE sigue siendo una forma eficaz y sofisticada de las organizaciones delictivas para lavar ganancias ilícitas;
2. Los investigadores federales, junto con agencias federales como la FinCEN y el IRS-CI han demostrado su capacidad para identificar y dismantelar o interrumpir determinados regímenes de BMPE; y
3. Sobre la base de las tendencias recientes de la fiscalía, parece que el DOJ seguirá enjuiciando enérgicamente a aquellos que no cumplan con las leyes de ALD destinadas a proteger la seguridad del público estadounidense, mantener la integridad de los mercados financieros estadounidenses, y, sin darse cuenta o no, realizan transacciones financieras que promueven o encubren delitos importantes que van desde el terrorismo, la toma de rehenes, la trata de personas y la distribución de drogas.

Historia de la trama del BMPE

El BMPE es conocido por haberse desarrollado en Colombia y surgió de la necesidad de los exportadores colombianos—tales como los que venden café, esmeraldas, o flores en los EE.UU.—de convertir los dólares ganados de la venta de estos bienes en pesos que los exportadores podrían utilizar en Colombia. En lugar de repatriar los dólares a través de medios legítimos, tales como cuentas bancarias, y por lo tanto enfrentar costos, tales como honorarios de transferencia, tipos de cambio, o impuestos, los exportadores colombianos utilizaban a alguien conocido como un corredor de pesos que compraba los dólares en los EE.UU., los depositaba en una cuenta bancaria de los EE.UU., y, a su vez, pagaba al exportador colombiano en pesos en Colombia.¹

Evolución del BMPE

Los corredores de pesos ya estaban dando servicio a los exportadores colombianos y tenían un sistema bancario bien desarrollado “paralelo” que también podía ser utilizado por los importadores colombianos que necesitaban acceso a dólares estadounidenses. Dichos importadores colombianos necesitan dólares para pagar el negocio de los EE.UU por los productos exportados a Colombia.

Como esta forma de la banca subterránea evolucionó, los importadores mexicanos también comenzaron a utilizar el esquema de BMPE para pagarles a las empresas estadounidenses en dólares y los corredores de pesos comenzaron a contratar a las organizaciones de tráfico de drogas (DTO, por sus siglas en inglés) que tenían grandes sumas de dólares en los EE.UU., que podían ser vendidos por los corredores de pesos a cambio de pesos.

¹ Véase, de manera general, “The Black Market Peso Exchange: How U.S. Companies are used to Launder Money,” 106th Congr. 60-125 (21 de junio, 1999).

Descripción general del sistema de BMPE

Una trama de BMPE puede darse en diferentes formas y variantes. En su forma más simple, se reduce a la ley de oferta y demanda:

1. Existe un suministro de ganancias ilícitas en los EE.UU. propiedad de una empresa delictiva extranjera que busca blanquear ese dinero. Por ejemplo, una organización de narcotráfico extranjera vendería cocaína en los EE.UU. a cambio de dólares.
2. A la DTO extranjera le gustaría usar esas ganancias en su país sin correr el riesgo de confiscación o robo por medio del contrabando de dinero u otros medios evidentes.
3. Esa DTO extranjera contacta un intermediario de pesos en el mismo país extranjero quien localiza un comprador de los dólares.
4. Los compradores adecuados de dichos dólares incluyen los importadores extranjeros que compran bienes de las empresas estadounidenses, que necesitan dólares, pero preferirían no pagar los costos de los fondos de transferencia por medio de cuentas bancarias, que podrían incluir tasas e impuestos adicionales.
5. El corredor de bolsa de pesos ofrece sus servicios tanto a la DTO como al importador mediante el pago de dólares al negocio de los EE.UU. de parte de la DTO en beneficio del importador. Una vez que el importador confirma que los dólares se han acreditado a la cuenta del importador en el negocio de los EE.UU., el importador paga el valor de esos dólares en pesos al corredor de pesos.
6. Una vez que el corredor de bolsa recibe pesos de parte del importador, el broker de pesos le paga a la DTO en pesos por los dólares comprados proporcionados a la empresa de los EE.UU.

Cómo se depositan ganancias ilícitas en el sistema bancario de los EE.UU.

Desde el punto de vista del ALD, el punto crítico en una trama de BMPE es cuando los dólares se acreditan en la cuenta del importador extranjero en la empresa de los EE.UU., porque es cuando surgen las banderas rojas.

Una empresa de los EE.UU. obtiene dólares de un importador extranjero de varias maneras diferentes, incluyendo: (a) la entrega por una persona no identificada que participa en la recogida y el movimiento del dinero ilícito; (b) recogida de dinero en efectivo por un empleado de la empresa estadounidense en un lugar de fácil acceso (es decir, estacionamiento, restaurante, garaje, almacén y cualquier negocio relacionado); (c) el depósito de dinero en efectivo (típicamente estructurado) en la cuenta bancaria de la empresa de los EE.UU.; y (d) las transferencias electrónicas a la cuenta bancaria de empresas estadounidenses financiadas por depósitos en efectivo estructurados.

Por su parte, la empresa de los EE.UU. puede estructurar el dinero en efectivo que aceptó físicamente en su negocio con el fin de eludir la obligación de informar sobre las transacciones monetarias. Alternativamente, se puede acumular el dinero en efectivo o utilizar los servicios de empresas de servicios de dinero (MSB), tales como los casinos, para lavar aún más el dinero.

Las leyes de BSA y AML violadas

La colocación de dólares mencionada, por lo general implica las siguientes violaciones de BSA/AML:

- La no presentación de un Formulario 8300 del IRS por parte de cualquier persona que recibe más de 10.000 dólares en una transacción o una serie de transacciones relacionadas, cifra debida a la realización de su actividad comercial o empresarial;
- Subdividir el efectivo y estructurar los depósitos en moneda (es decir, hacer múltiples depósitos de no más de \$10.000 en efectivo para evadir la presentación de un informe sobre las transacciones monetarias [CTR] por una institución financiera);
- La recepción de dinero en efectivo de personas desconocidas y el posterior desembolso a otro individuo o negocio en los EE.UU. (es decir, el funcionamiento de una empresa de transmisión de dinero sin licencia);
- Igual que el anterior, sin embargo, el desembolso posterior se podría hacer por transferencia bancaria o cheque;
- La creación de múltiples capas en una transacción financiera para evadir los requisitos de información y ocultar el origen de los fondos. Por ejemplo, si una empresa de los EE.UU. acepta más de \$10.000 en efectivo, esa empresa puede estructurar los depósitos en moneda en su cuenta bancaria para evadir los CTR. Alternativamente, podría abrir varias cuentas en las que se hicieran múltiples depósitos de no más de \$10.000 en efectivo; y
- Cuentas bancarias de empresas reciben transferencias financiadas por depósitos en efectivo estructurados en la institución financiera que hizo la transferencia bancaria.

Casos recientes de BMPE

Los siguientes son los casos presentados entre 2010 y 2014 contra las corporaciones que participan en tramas de BMPE:

- En *Estados Unidos vs. Angel Toy Corp., et al.*, CR No. 10-718 (C.D. Cal 2010), Angel Toy Corp. fue acusado de conspirar para estructurar las transacciones financieras, el contrabando de dinero en efectivo, el blanqueo de dinero, la manipulación de un testigo y la estructuración de la exportación de instrumentos monetarios. Los propietarios se declararon culpables de conspirar para estructurar las transacciones financieras y fueron condenados a 37 meses de prisión y la empresa recibió la orden de entregar \$1 millón. De acuerdo con los documentos de la sentencia, más de \$8 millones fueron canalizados a cuentas bancarias de Angel Toys durante un período de cuatro años, y cada depósito fue por menos de \$10.000 para evitar los requisitos de presentación de informes.
- En *Estados Unidos vs. Woody Toys, Inc. et al.*, CR No. 12-329 (C.D. Cal. 2012), sin inmutarse, los dueños de Woody Toys, Inc. contrataron a los empleados de Angel Toys Corp. y procedieron a realizar negocios con los clientes anteriores de Angel Toys en Colombia y México. Woody Toys, sus dueños, tres empleados y dos clientes mexicanos fueron acusados de conspirar para evadir los requisitos de presentación de informes y el blanqueo de dinero, y se cree que lavaron por lo menos \$6 millones en seis años. La acusación alega que un cliente mexicano compró “narcodólares”, que es la forma en que fue capaz de obtener un tipo de cambio más barato para los dólares estadounidenses. Ese cliente mexicano y Woody Toys se declararon culpables de conspirar para lavar dinero, mientras que el dueño y los empleados se declararon culpables de conspirar para evadir los requisitos de presentación de informes financieros. Los propietarios recibieron una condena colectiva de 38 meses y a la empresa se le decomisó \$2 millones.

- En *Estados Unidos vs. Peace & Rich Import, Inc., et al.*, CR 13-107 (C.D. Cal. 2013), el dueño de una empresa de flores de seda fue acusado de conspirar para operar una empresa de dinero sin licencia, no entregar un CTR, la estructuración de las transacciones financieras y complicidad. El propietario fue condenado a 12 meses de prisión y admitió que él distribuyó más de \$1 millón en efectivo recibido en nombre de las empresas mexicanas a otras empresas en Los Ángeles durante un período de tres años. A la empresa se le decomisó \$2 millones.
- En *Estados Unidos vs. QT Fashion, Inc., et al.*, CR 14-372 (C.D. Cal. 2014), el propietario de la tienda de maternidad, el gerente y la empresa mexicana que presuntamente compró ropa de maternidad de QT Fashion, así como sus empleados, fueron acusados de conspirar para lavar dinero y operar una empresa de transferencia de dinero sin licencia. QT Fashion presuntamente aceptó dinero del rescate que llevó a la liberación de un ciudadano estadounidense retenido como rehén y torturado por una organización de narcotráfico en México. La acusación formal también alega una conspiración para el contrabando de mercancías de los EE.UU. por la alteración de las etiquetas de la ropa de “Made in China” a “Made in America”, con el fin de obtener un trato fiscal preferencial en virtud del Acuerdo de Libre Comercio de América del Norte.
- En *Estados Unidos vs. Pacífico Eurotex Corp., et al.*, CR No. 14-521 (C.D. Cal 2014), los propietarios y empleados de la empresa textil con clientes en México, Guatemala, Colombia y Perú, fueron acusados de conspirar para lavar dinero, la estructuración de las transacciones monetarias y de no presentar los CTR que se requieren de un comercio o empresa no financiera.
- En *Estados Unidos vs. Xilin Chen, Chuang Feng Chen, y Aixia Chen*, CR No. 14-499 (C.D. Cal 2014), los propietarios de dos compañías diferentes de ropa interior, fueron acusados de conspirar para lavar instrumentos monetarios, que presuntamente fueron producto del tráfico de estupefacientes, así como violaciones relacionadas con la inmigración.

¿Cómo son vulnerables las instituciones financieras y los MSB a tramas de BMPE?

Las instituciones financieras y las MSB también pueden ser vulnerables a las tramas del BMPE. Como “guardianes”, deben ser conscientes de los siguientes:

- Sobre la base de algunos de los casos mencionados anteriormente, los depósitos en efectivo anónimos estructurados de fuera del estado se hicieron en las cuentas bancarias de los EE.UU. Los bancos deben estar atentos y presentar reportes de operaciones sospechosas (ROS) en la detección de dicha actividad. Para hacerlo, los bancos tienen que entender los negocios de sus clientes y las regiones geográficas pertinentes como parte de su política de conozca a su cliente (KYC).

Los bancos tienen que entender los negocios de sus clientes y las regiones geográficas pertinentes como parte de su política de conozca a su cliente (KYC)



- Por otra parte, los bancos deben seguir presentando un CTR cuando se deposita más de \$10.000 en efectivo en una cuenta bancaria. Los empleados del banco también deben ser advertidos de no asesorar a los clientes existentes y potenciales de la política de informes de CTR, que anima a la estructuración.
- Los bancos también deben presentar CTR y ROS cuando se observan los patrones de los depósitos en moneda estructurados, así como “micro-estructuración”, que son los múltiples depósitos de moneda en cantidades que van desde aproximadamente \$2.500 a \$5.000, especialmente cuando el titular de la cuenta es una empresa estadounidense que exporta a México, América Central y del Sur, o a cualquier país sancionado por los EE.UU.
- En los extractos de cuenta del cliente, la ubicación (ciudad, estado) de los depósitos en moneda deben señalarse, lo que informaría al titular de la cuenta bancaria de cualquier actividad inusual que puede requerir escrutinio.
- Los bancos pueden presentar ROS cuando una cuenta abierta en un estado (en particular a lo largo de la frontera suroeste) recibe múltiples depósitos en efectivo de no más de \$10.000 por parte de personas no identificadas en sucursales fuera de la región geográfica en la que está domiciliada la cuenta.
- Los bancos con sucursales en México, América Central y del Sur, o de cualquier país sancionado por los EE.UU., deben desarrollar, mantener y hacer cumplir las políticas de ALD, así como implementar programas de computación destinados a la detección de patrones donde se depositan grandes cantidades de dinero en efectivo en una cuenta bancaria fuera de los EE.UU., cuyos fondos son entonces conectados a una cuenta diferente en los EE.UU.
- El modelo anterior también podría implicar el uso de las cuentas bancarias de corresponsalía donde las transferencias electrónicas a los exportadores de los EE.UU. pasan a través de la cuenta corresponsal del Banco A México con el Banco A EE.UU. Del mismo modo, los dólares de la droga que se depositan en el Banco A México se pueden vender a través del Banco A EE.UU. por medio de billetes de banco.
- Las instituciones financieras también deben informar en los ROS y/o CTR la denominación de la moneda de los EE.UU. depositada en cuentas bancarias porque, tradicionalmente, el tráfico de drogas en un nivel de la calle produce billetes más pequeños tales como \$1, \$5, o \$20.
- Los bancos con sucursales o filiales en otros países deben adherirse a las normas de ALD de los EE.UU. y la racionalización de los informes internos de tal manera que el oficial de cumplimiento más alto tiene una supervisión directa sobre todos los oficiales globales de cumplimiento.

- Los bancos deben monitorear cuidadosamente la actividad de las cuentas sospechosas, tales como múltiples cuentas abiertas el mismo día o en poder de los mismos ciudadanos extranjeros en diferentes bancos; cuentas bancarias que permanecen en estado latente durante largos períodos de tiempo, seguido de la actividad bancaria espuria en la que se hacen grandes transacciones o transacciones estructuradas; y el aumento de la frecuencia y las cantidades de los depósitos en moneda por parte de empresas de exportación de los EE.UU.
- Por otra parte, las MSB, como casinos, igualmente deben ser conscientes de las tramas del BMPE, porque los participantes del BMPE (correos postales o dueños de negocios/empleados) pueden cambiar billetes de denominación más pequeñas a las de denominación más grande, que pueden ser depositados en un banco o transformados en un cheque o transferencia.

Conclusión

Es razonable creer, sobre la base de la historia y la evolución del BMPE, que esta trama compleja persistirá y tal vez se hará aún más sofisticada a través de la creación de capas adicionales en una operación financiera diseñada para ocultar el origen de los fondos ilegales.

La comunidad de ALD puede esperar ver más actividad de aplicación de la ley que implica leyes de BSA/ALD y aumento de la actividad reguladora. FinCEN puede emitir más orientación con respecto a la presentación de formulario del IRS 8300s, CTR, ROS, ya que se ha publicado recientemente una guía sobre CMIR. Como resultado, las empresas y las instituciones financieras deberían revisar sus políticas internas de ALD; proporcionar formación a los empleados sobre las tramas de lavado de dinero sofisticadas, como el BMPE, las tendencias y regulaciones federales y estatales informadas; designar oficiales de cumplimiento adecuados y aplicar una estructura de información adecuada que proporciona la rendición de cuentas en relación con el cumplimiento de BSA/ALD y la formación con la supervisión de una comisión de la junta directiva; y gastar en recursos que ejecutan los programas encaminados a detectar y reportar actividades sospechosas. **A**

Christine S. Bautista, socia, Litigation Practice Group/White Collar and Internal Investigations, Akerman LLP, Chicago, IL, EE.UU., christine.bautista@akerman.com

Desechando el cuero para confeccionar

una billetera electrónica



Desde la primera vez que una persona le dijo a otra: “Quiero eso que tienes”, ha habido necesidad de moneda fiable. Inicialmente, esa moneda consistía en un sistema de trueque en el que se negociaban bienes y/o servicios. Eventualmente esto pasó a monedas, que a su vez evolucionaron hasta convertirse en un sistema basado en papel plástico y luego tarjetas de crédito y de débito. Cada cambio se ha hecho para que los involucrados tuvieran una experiencia transaccional más práctica y segura. Hoy en día, el mercado es testigo de una evolución sin precedentes a moneda digital que cambia no sólo lo que la gente compra, sino dónde compra y cómo paga. En el centro de este cambio radical se encuentra un sistema que permite que la moneda digital cambie de manos: billeteras digitales o billeteras electrónicas.

Proteger la información del uso y abuso de parte de los criminales es un proceso permanente y un esfuerzo continuo

Teniendo en cuenta lo tecnológicamente avanzada de la humanidad de hoy, es algo sorprendente que todavía llevemos billeteras de cuero (y carteras) con todo tipo de tarjetas plásticas, cupones, monedas y mucho más. Ahora mismo estamos empezando a entender cómo convertir esto en un formato digital, que añade las mejoras que uno esperaría en el proceso de conversión. Los consumidores son inteligentes y no adoptarían una billetera digital torpe con menos utilidad que su billetera física. En el mundo altamente competitivo en el que las aplicaciones (apps) están compitiendo por la atención del consumidor, el mercado ha llegado a esperar (si no incluso exigir) mejoras significativas antes de interesarse por una aplicación en línea.

Las billeteras electrónicas permiten moneda digital

Mucho antes de que se utilizaran tarjetas de pago (es decir, de débito, de crédito, de regalo y tarjetas de fidelidad) y cheques para los pagos, se utilizaron monedas. Curiosamente, como surgió la Internet, las formas de pago más obviamente adecuadas para un mundo electrónico se aceleraron, mientras que las monedas nacionales se quedaron atrás. La moneda sigue teniendo una historia diferente. La manera de hacer que funcione la moneda de manera electrónica preservando los atributos que hacen funcionar las monedas tan bien (es decir, la inmediatez de pago, la conclusión de pagos y la privacidad del pago por nombrar algunos) no era tan obvio. Sin embargo, la comprensión de cómo hacer que las monedas trabajen electrónicamente está comenzando a emerger.

Por ejemplo, sólo en los últimos años ha habido informes de noticias de bitcoin y otra moneda digital que hacen su camino en el mercado. Las

empresas que desarrollan el protocolo Bitcoin han recaudado millones de dólares validando interés empresarial en resolver este problema.

Una billetera electrónica puede contener elementos parecidos a una cartera de piel tales como tarjetas de identificación (por ejemplo, licencias de conducir digitales), cupones, monedas nacionales (es decir, dólares, euros, pesos mexicanos), tarjetas (de débito y crédito, de regalo, de fidelización, de recompensas). El propósito de una billetera electrónica es no sólo crear una ubicación de almacenamiento electrónico para mantener estos tipos de artículos, sino también para añadirles inteligencia a lo que simplifica nuestras vidas. Por ejemplo, una billetera electrónica avanzada sabrá cuando uno está haciendo un pago a un establecimiento comercial específico por lo que le puede pedir al usuario que canjee el valor en una tarjeta de regalo (ya no habrá más preocupaciones acerca de olvidar las tarjetas de regalo), puede capturar automáticamente el valor de fidelización aplicable a la compra sin necesidad de presentar una tarjeta de fidelización específica. También le puede pedir la redención de un cupón en la billetera. La billetera electrónica puede también presentarles a los consumidores actuales las ofertas en sus tiendas favoritas por medio de un programa de marketing en línea.

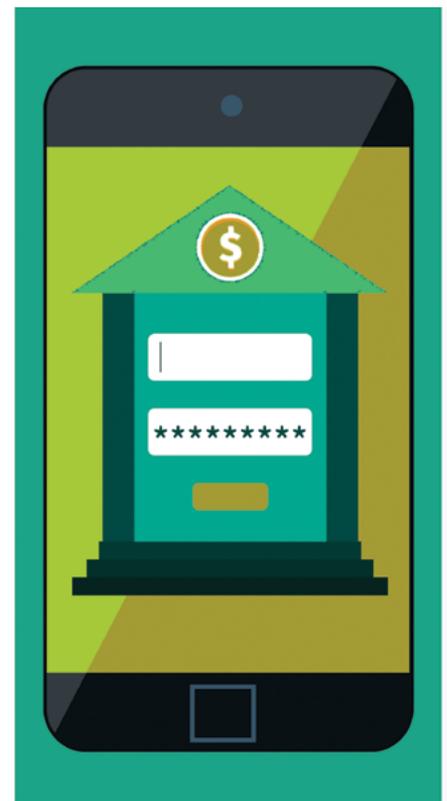
Aunque técnicamente las billeteras electrónicas se pueden utilizar a nivel internacional, los países individuales pueden tener leyes y regulaciones sobre el uso de la moneda, tarjetas de pago (por ejemplo, tarjetas de débito y de crédito) y la redención de tarjetas de regalo, tarjetas de fidelización y cupones. Estas leyes y regulaciones pueden aplicarse incluso cuando se utiliza una billetera electrónica para mantener estos elementos de forma digital. También estamos viendo que los reguladores anuncian resoluciones adicionales que se refieren específicamente a la moneda digital. Por ejemplo, la Red Contra los Delitos Financieros (FinCEN) emitió resoluciones administrativas en enero con respecto a las operaciones mineras de moneda virtual y desarrollo de software de moneda virtual y actividades de inversión. Una de las responsabilidades de un oficial de cumplimiento es reforzar las normas y reglamentos de la organización.

Por otra parte, algunos países extranjeros menos desarrollados se encuentran en realidad adelantados en la adopción de la moneda digital porque la seguridad y la comodidad

se magnifican y representan una mejora tan convincente. Mientras que los EE.UU. ha sido un líder en infraestructura de pagos, está viendo que otros países se adelantan debido a su rápida adopción de tecnologías móviles, monedas digitales y el entorno regulatorio menos desarrollado.

Detectando las debilidades

Proteger la información del uso y abuso de parte de los criminales es un proceso permanente y un esfuerzo continuo. La industria constantemente busca maneras de mejorar la integridad de los sistemas de pago digitales incluyendo las billeteras electrónicas. Un ejemplo actual es el reciente anuncio por parte de Apple de Apple Pay. Apple Pay elimina los números de cuenta de tarjetas de pago convirtiendo en tokens (indicios o datos, en español) el número de tarjeta de pago. Un número de tarjeta de pago hecho token es una cadena de dígitos que se vuelven sin sentido cuando se extraen de su contexto seguro. Apple Pay también aprovecha la tecnología de identificación táctil de un teléfono móvil para validar el pagador. La validación de la persona que está haciendo el pago es un paso importante en la protección de

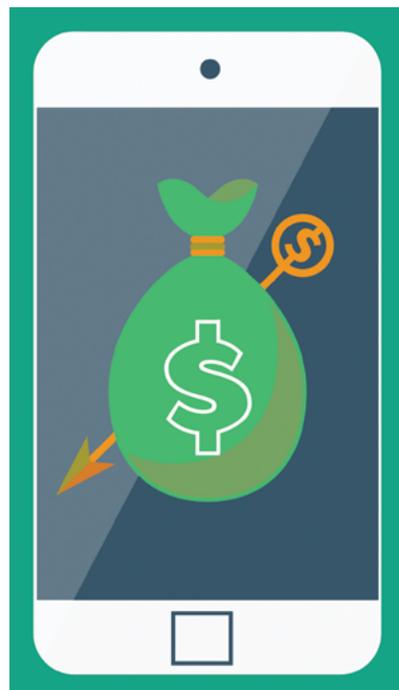


La validación de la persona que está haciendo el pago es un paso importante en la protección de la integridad del sistema de pagos

la integridad del sistema de pagos. Una billetera electrónica no está sola. Se debe tener en cuenta la seguridad desde el principio con el fin de mantener la confianza. Por ejemplo, la transparencia y la privacidad son elementos críticos en la construcción de confianza. Cada transferencia de una moneda nacional entre las billeteras electrónicas implica tres partes: proveedor o emisor de la moneda nacional (por ejemplo, una institución financiera aquí en los EE.UU.), un pagador y el beneficiario. La transparencia significa que las partes interesadas en la transferencia de la moneda nacional tengan acceso adecuado a la información para apoyar sus funciones y responsabilidades a la vez que se mantiene la privacidad. La seguridad y el control son también fundamentales para construir confianza. Una billetera electrónica ofrece una oportunidad para mejorar tanto la seguridad como el control simplemente invirtiendo cómo se lleva a cabo una transferencia. Al permitir que los consumidores empujen el pago a la billetera electrónica del comerciante en lugar de que el comerciante lo tome de la billetera electrónica del consumidor, el control del pago es devuelto al consumidor, lo que también aumenta la seguridad para el consumidor y el comerciante. Una billetera electrónica permite que las transferencias se completen sin que el comerciante tenga que proteger las cuentas de pago de los consumidores (por ejemplo, número de tarjeta de débito, número de tarjeta de crédito).

La seguridad es un proceso iterativo común, continuo de identificación de posibles puntos débiles y de su fortalecimiento frente a usos inadecuados y abusos. La seguridad es integral e importante desde una perspectiva sistémica. Mover dinero en efectivo a un sistema de billetera electrónica en la nube garantiza el pago de las maneras que antes eran más difíciles o ni siquiera posibles. Por ejemplo, la preservación de la naturaleza portadora de una moneda nacional como el dólar estadounidense y el anclaje electrónico de cada factura, independientemente de la denominación, a

una dirección Web única se convierte en una forma de verificación de parte del público para verificar la autenticidad del instrumento de pago. Cuando todos los que participan en el sistema de monedero electrónico pueden fácilmente verificar la integridad de un instrumento de pago, entonces se incrementa la confianza colectiva en el sistema. El gobierno federal publica información y fomenta la educación pública acerca de las características de seguridad del nuevo billete de \$100 para que todo aquel que acepte billetes de 100 dólares no sea engañado fácilmente por una falsificación. Cuando las características de seguridad del instrumento de pago son difíciles o incluso imposibles de copiar, sino que también son fácilmente identificables y verificables por cualquier persona que utilice el sistema, incluyendo el oficial de cumplimiento, la confianza colectiva en el sistema aumenta. Los fieles a Bitcoin rápidamente



se refieren a la importancia del anonimato como una característica de la moneda digital; sin embargo, también es importante poder visualizar y verificar independientemente la autenticidad del instrumento de pago y sus características de seguridad tal como podemos con las facturas físicas.

La manera en la que el oficial de cumplimiento pueda mitigar el riesgo de una moneda digital consiste en descartarlo. El oficial de cumplimiento debe estar preparado para debatir en reuniones y debe haber identificado razones demasiado arriesgadas para la organización en participar con una moneda digital directa o indirectamente. En lo que respecta a la utilización de la moneda digital, no es el trabajo del oficial de cumplimiento promover su uso, eso corresponde a la empresa. Haga eso para lo cual usted ha sido contratado: diga “no”. Siga diciendo “no” hasta que la seguridad y la solidez de la moneda digital hayan sido controladas adecuadamente en el mercado.

Cuando la moneda digital se encuentra más segura

Un instrumento de pago digital es en sí más seguro cuando las características de autenticidad y de seguridad del instrumento de pago se comparten públicamente, y son visual e independientemente verificables. Las transferencias mediante un instrumento de pago digital seguro se hacen más seguras cuando se realizan cuando hay un seguimiento de posesión, grabado, transparencia y es privado. Una billetera electrónica debe ser digna de confianza por parte del consumidor, el comercio electrónico y al nivel de institución financiera para tener éxito a largo plazo. La seguridad de la moneda digital es un conjunto completo de atributos, características y funciones que trabajan juntos en un sistema de billetera electrónico para construir y mantener la integridad y la confianza del sistema.

Durante décadas, la billetera física fiable ha sido el hogar de las tarjetas de pago (por ejemplo, de débito/crédito), tarjetas de regalo/de fidelización, cupones y efectivo y ha funcionado bien, pero la evolución ha comenzado y no hay nada que la detenga ahora. Las billeteras electrónicas se están construyendo sobre la aceptación de cómo y por qué funcionan en una experiencia digital que simplifica la forma en que se utilizan estos artículos en línea en un mundo móvil para mejorar la vida aún más. **TA**

Bradley Wilkes, fundador y CEO, WingCash, Highland, UT, EE.UU., brad@wingcash.com

Celebrating 25 years as the world's leading financial crimes news source

Unmatched in its editorial coverage, with an archive of nearly 4,000 news articles, enforcement action updates, and country-specific legislation, ACAMS moneylaundering.com is regularly the first to break critical news compliance professionals rely upon to protect their financial institutions.

The screenshot shows the ACAMS Money Laundering.com website homepage. The browser address bar displays 'www.moneylaundering.com/Pages/Home.aspx'. The website header includes the ACAMS logo and navigation links for 'About Us', 'Contact Us', 'Features', 'acams.org', and 'Login'. A secondary navigation bar contains 'Home', 'Legs & Regs', 'News', 'Enforcement Actions', 'Countries', and 'Resources'. The main content area is divided into several sections:

- News »**: Contains articles such as 'For Growing Digital Currency, Regulatory Scrutiny Has Coincided with Investor Interest' (dated August 23, 2013), 'Weekly Roundup: U.S. Military Researches Use of Twitter Data to Identify Laundering, Ocean Bank DPA Ends, and More' (dated August 23, 2013), 'Following New York State Settlements, Some Foreign Banks Consider Charter Shopping' (dated August 22, 2013), and 'Midweek Roundup: German Regulator Probes Alleged Deutsche Bank AML Violations, Mexican Kingpin Gets 15 Years, and More' (dated August 21, 2013).
- Legs & Regs »**: Contains articles such as 'U.S. Attorney's Office Co-Sponsors Ninth Annual Counterterrorism and Financial Crimes Forum' (dated August 22, 2013), 'Sierra Leone Man Charged with Brokering Supply of Uranium to Iran' (dated August 22, 2013), and 'India's Regulator Publishes 2012-2013 Annual Report' (dated August 22, 2013).
- Test Your AML IQ**: A section with a title 'According to the Inter-Governmental Action Group Against Money Laundering in West Africa (GIABA), red flag indicators for tax crimes and money laundering include:' followed by two multiple-choice options:
 - A. Ostentatious and conspicuous lifestyles and sudden unexplained wealth.
 - B. Former tax officials working as tax consultants for corporate high net worth companies.
- ACAMS moneylaundering.com's Complimentary Article**: A featured article titled 'Many Financial Institutions Unlikely to Meet FinCEN's E-Filing Deadline' with a 'Download Today!' button.
- From the Editor »**: A section titled 'From the Editor: What's Up with Russia?' discussing anti-money laundering enforcement actions against financial institutions in Russia.
- Enforcement Actions »**: A section titled 'Warning: Promregionbank Must Address AML/CTF Deficiencies (in Russian)' with a 'Read More' link.

At the bottom of the page, there are buttons for 'CONFERENCES', 'SEMINARS', and 'WEBINARS', and a 'Subscribe Now' button for a free email newsletter.

SUBSCRIBE NOW!

moneylaundering.com

RECONOCIMIENTO *a la Clase* DE 2014

A *CAMS Today* querría felicitar a todos los ganadores de los premios del 2014. Hasta ahora, la Clase de 2014 ha sido la más grande. Tuvimos seis ganadores individuales y también al ganador del Capítulo del Año. *ACAMS* se encuentra orgullosa de todos nuestros socios que ayudan a hacer de *ACAMS* una asociación de primer nivel. Nos gustaría aprovechar este momento para agradecerles públicamente a todos ustedes por sus contribuciones continuas a *ACAMS*.



Por primera vez, nos gustaría presentar a los ganadores de los premios de nuestra Clase de 2014 a todos nuestros miembros.

Felicidades a:

KEVIN ANDERSON, Voluntario Al Gillum del Año

BRIAN ARRINGTON, Artículo del Año

CLAYTON BYFORD, Artículo del Año

CAROL STABILE, Artículo del Año

MICHAEL MCDONALD, Premio Pioneer de ALD

CHUCK TAYLOR, Profesional del Año de ALD

CAPÍTULO DE ACAMS DE MONTRÉAL, Capítulo del Año

ACAMS Today tuvo la oportunidad de entrevistar a los ganadores de los premios junto con dos miembros de la junta asesora del Capítulo de Montreal, Sylvain Perreault y Éric Lachapelle. La entrevista cubre temas que van desde la forma en que entraron en el campo de la prevención de ALD/delitos financieros a las predicciones sobre los retos de la industria a los que nos enfrentaremos en 2015. El conocimiento, la experiencia y la sabiduría de estos ganadores es de gran alcance, por decir lo menos. Espero que usted disfrute de conocer a los ganadores tanto como yo disfruté entrevistarlos.

ACAMS Today: ¿Qué lo inspiró a entrar al campo de la prevención del delito financiero?

Kevin Anderson: No diría que haya sido una noble inspiración; mi primera oportunidad en el campo de ALD fue sobre todo una cuestión de buena suerte. Fue tentador en que ofrecía más posibilidades de ascenso y presentaba más desafíos que mi trabajo anterior en la administración de fideicomisos. También había una sensación de que, en los años de trabajo antes de la promulgación de la Ley del Patriota, se estaba haciendo algo para combatir la delincuencia y hacer de la comunidad un mejor lugar en vez de sólo servir a los clientes y ayudar a ganar más dinero.

Brian Arrington: Mi entrada en la prevención del delito financiero fue un hecho “accidental”. Entré en el sector de los servicios financieros a mediados de la década de 1990 como analista temporal de fraude de tarjeta de crédito en un banco importante de la costa este. Con el tiempo, fui contratado a tiempo completo y encontré el trabajo tan interesante y diverso, desde las solicitudes fraudulentas masivas y el robo de correo hasta tarjetas falsificadas que simplemente seguí mis intereses. A partir de ahí, aproveché mi experiencia previa y profundicé en la industria en transacciones y análisis de riesgo de la cartera y en última instancia las investigaciones de fraudes de crédito, trabajando indirectamente con profesionales de la ley experimentados.

En estos papeles posteriores tenía una mirada de primera mano en el aumento de las principales tendencias y técnicas, tales como tramitas de fraudes de tarjetas, esquemas de monetización y envío; robo de identidad; apropiación de cuentas; fraude por correo; falsificación y “skimming”; y el fraude de crédito organizado por Internet. Esta fue también mi primera exposición a los ROS y el proceso de presentación de ROS. Salí de la industria de tarjetas de crédito durante varios años, mientras trabajaba para una de las tres agencias de crédito de los EE.UU. Estados Unidos, pero nunca olvidé esta exposición a la delincuencia financiera y su impacto en el consumidor medio y el sistema bancario de EE.UU.

Finalmente volví a la banca en un papel de cumplimiento de ALD en un gran banco de los EE.UU. justo después de terminar mis estudios de MBA, y aunque no me di cuenta en aquel momento, las bases de mi entrada en la profesión de ALD se prepararon durante esos primeros años en la industria de tarjetas de crédito.

Clayton Byford: Mi inspiración para unirme a la comunidad financiera de contra amenazas fue realmente una evolución en la trayectoria profesional de algunos de mis trabajos en la lucha contra el terrorismo en Afganistán y mi experiencia apoyando investigaciones antinarcoóticos de la policía. Un tema común siempre ha sido identificar los grupos u organizaciones que representan una amenaza y, a continuación, identificar cómo y dónde son vulnerables. La contra amenaza de finanzas se centra específicamente en una de las dos áreas donde estos grupos son más vulnerables: pagos y comunicaciones. Me gusta trabajar en este campo debido a la complejidad; siempre exigente y siempre cambiante, tanto para nosotros como para los que deseen utilizarla para apoyar organizaciones ilícitas.

Michael R. McDonald: Fue lo que escogí como carrera. En 1971 con una licenciatura en contabilidad y no queriendo ser contador, entré a lo que entonces se llamó la División de Inteligencia del IRS. Más tarde el nombre



ARTÍCULO DEL AÑO

Carol Stabile, CAMS

Carol Stabile entró a Safe Banking Systems (SBS) en 2006 como gerente de negocios senior con la responsabilidad de clientes globales y desarrollo estratégico de productos y servicios. Su papel se amplió hasta incluir políticas operativas de SBS y gestión de proveedores. En su función de marketing, Stabile ha remarcado los productos y servicios de SBS, gestiona eventos de SBS y es colaboradora habitual de *ACAMS Today* y otras publicaciones del campo.

Stabile es ex banquera internacional con más de 25 años de experiencia tanto en operaciones como en la tecnología de la empresa. Ha dedicado una parte importante de su carrera al trabajo en el extranjero en Asia, Europa, América Latina y las Bermudas. Obtuvo una licenciatura de Pace University, Nueva York y ha sido profesora de Operaciones de Banca Internacional en la American Institute of Banking en Nueva York. En 2008 Stabile recibió su certificación CAMS.



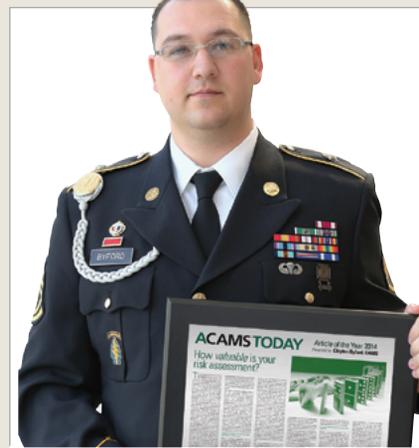
ARTÍCULO DEL AÑO

Brian Arrington, MBA, CAMS

Brian Arrington es examinador en el Banco de la Reserva Federal de Chicago. Tiene más de 15 años de experiencia en la industria de servicios financieros, con extensa exposición a las regulaciones de cumplimiento por medio de una amplia gama de instituciones. Antes de entrar al Banco de la Reserva Federal, Arrington fue consultor de gestión de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD) y Oficina de Control de Activos Extranjeros (OFAC) en cuestiones de cumplimiento normativo para una empresa de contabilidad del "Big 4", donde prestó servicios de asesoramiento a las grandes instituciones financieras complejas.

Anteriormente, Arrington fue oficial de cumplimiento encargado de BSA/ALD y OFAC de un banco grande en el área de Chicago, donde dirigió las investigaciones de BSA/ALD, los procesos de cumplimiento de la OFAC y las iniciativas clave del programa de cumplimiento de BSA/ALD/OFAC.

Arrington tiene un certificado de CAMS, es director de comunicaciones de la junta directiva del Capítulo de ACAMS de Chicago, y miembro tanto del Grupo de Trabajo Editorial como de los Grupos de Tareas Educativas de ACAMS. Obtuvo su doble MBA de la Escuela de Negocios Kellstadt de la Universidad DePaul en economía internacional y gestión empresarial.



ARTÍCULO DEL AÑO

SFC Clayton Byford, CAMS

SFC Clayton Byford es un analista financiero en contra amenazas del Grupo de Tareas Antidrogas de la Guardia Nacional del Ejército de Illinois. Está actualmente asignado al Área de Alta Intensidad de Narcotráfico de Chicago (HIDTA), Centro de Apoyo de Inteligencia y al Área de Alta Intensidad de Delitos Financieros y Lavado de Dinero (HIFCA) bajo la Red Contra los Delitos Financieros (FinCEN). Tiene más de 10 años de experiencia como analista de inteligencia militar con dos periodos de combate en Afganistán. Byford ha estado activo en la lucha contra los estupefacientes en los últimos siete años, los tres últimos de los cuales se centraron específicamente en el ALD, delitos financieros y la inteligencia financiera. Byford es un Especialista Certificado en Antilavado de Dinero (CAMS).

Me gusta trabajar en este campo debido a la complejidad; siempre exigente y siempre cambiante

fue cambiado a División de Investigación Delictiva. He trabajado en el campo de Delitos Financieros desde entonces.

Sylvain Perreault y Éric Lachapelle:

Para evitar que unas pocas manzanas podridas echen a perder una industria respetable y bien regulada al servicio de toda la comunidad.

Carol Stabile: Como ex banquera internacional y jefa de operaciones de Asia Pacífico para un banco de los EE.UU., mis responsabilidades incluían el cumplimiento regulatorio. También tuve varios miembros de la familia que perseguían carreras en aplicación de la ley, por lo que cuando la oportunidad llegó para trabajar para una empresa a la vanguardia de la prevención del delito financiero, me sentí emocionada de formar parte de ese esfuerzo.

Chuck Taylor: Como muchos otros en el campo caí en ella fortuitamente. A los 29 años, mientras trabajaba para el Bank of America, decidí que quería ser fiscal, así que fui a estudiar derecho y trabajé como pasante de un fiscal adjunto que estaba a cargo de los casos de delitos sexuales y abuso infantil. Me gustó mucho la escuela de derecho y ayudar a poner a los malos adentro, pero al final de mi pasantía había decidido que el trabajo no era para mí. Como se pueden imaginar, las cosas que vi eran bastante inquietantes y difíciles de olvidar y no era algo de lo que quería hacer un trabajo de por vida. Volví a la banca como analista de cumplimiento (algo de lo que no sabía nada) a una institución pequeña en Santa Bárbara, California. Les habían dado los asuntos de la BSA que requieren la atención del OCC y necesitaban a alguien para ayudar con la remediación. En los próximos años labré mi camino y me convertí en oficial de BSA y me gustó mucho el trabajo. Tuve la suerte de caer en este campo, ya que ha sido increíblemente gratificante y me mantiene entretenido.

AT: Siempre están evolucionando las amenazas y los retos para el profesional de la delincuencia financiera, ¿qué prevé usted como el mayor reto del año que viene y cómo debería el campo de la delincuencia de ALD/financiera prepararse para resolverlo?

KA: El mayor desafío sigue siendo gestionar el cambio, si se trata de nuevos productos con nuevas vulnerabilidades, nuevos tipos de clientes que presentan riesgos que deben ser gestionados o nuevas expectativas regulatorias que deben gestionarse. Continúo

Es crucial, como profesionales de ALD, que entendamos mejor el impacto de la tecnología

admirándome de que 13 años después de la aprobación de la Ley del Patriota el ALD sigue siendo un tal tema de cumplimiento caliente, con nuevos problemas que surgen para mantener ocupados a los profesionales de ALD. La clave para manejar esto es ser ingenioso y flexible; tener un gran sentido del humor, paciencia y una piel gruesa.

BA: Yo creo que el crecimiento y la creciente sofisticación de la delincuencia organizada transnacional es la amenaza más grave para los EE.UU. y, en última instancia, para el sistema financiero global, tanto en la actualidad como en los años venideros. Desde una perspectiva de ALD y TF, creo que la amenaza de la delincuencia organizada transnacional ha sido permitida en gran medida por los avances tecnológicos en la forma de las comunicaciones por Internet y móviles, y es crucial, como profesionales de ALD, que entendamos mejor el impacto de la tecnología si queremos tener algún éxito en detener este problema.

Puede haber varias claves para mitigar esta amenaza. Lo primero es reconocer que es necesario un cambio de paradigma para reorientar los objetivos de prevención del delito financiero en combatir verdaderamente la delincuencia organizada transnacional. Sin una visión clara y el liderazgo de arriba hacia abajo, incluso los mejores esfuerzos de ALD son insostenibles. En segundo lugar, los profesionales de ALD deben tratar de avanzar hacia o conseguir estar a la vanguardia de la comprensión de la tecnología, tanto a nivel interno mediante la búsqueda de herramientas para ayudar de manera más eficaz las iniciativas de ALD, como externamente mediante una mejor comprensión de los usos duales que se manifiestan con cada nuevo avance tecnológico. En tercer lugar, y este asunto se discutió también en la conferencia de Las Vegas de este año, creo que las

deficiencias actuales en la legislación de ALD y los regímenes reguladores internacionales explotados por los delincuentes deben reducirse si la comunidad de ALD debe alcanzar cualquier grado de éxito en reducir al mínimo el impacto de fondos ilícitos en el sistema global de servicios financieros. Se necesitan cambios en las políticas a nivel mundial para ayudar a la comunidad de ALD si los EE.UU.—y en última instancia, la infraestructura de los servicios financieros internacionales—quiere sobrevivir en el corto y largo plazo.

CB: Las mayores amenazas que enfrentamos vienen de las organizaciones delictivas transnacionales. El curso de la información y las investigaciones que sobrepasan las fronteras internacionales es muy complicado, y esto es una ventaja para estas organizaciones. Al menos parte de la respuesta a esto es claro de definir: la mejor y más completa comunicación entre los gobiernos y las instituciones financieras ayudaría a comprender mejor el alcance de esta amenaza. Sin embargo, no es tan fácil de lograr.

ÉL: Tenemos que ser conscientes de las amenazas que vienen del mundo digital (monedas virtuales, nuevas aplicaciones móviles, etc.). Los especialistas de ALD tendrán que ser capacitados más sobre estos nuevos productos y servicios. ¡La clave es la formación!

MM: Tecnología. Por ejemplo, ¿dónde se comete un delito si se trata de uno cibernético? ¿Cómo se establece lugar si las transacciones son virtuales y globales en el mundo cibernético? Esto incluye la explosión de los métodos de pago que están más allá del alcance de mucha cobertura estatal y nacional (como FinCEN). Las necesidades profesionales de ALD tienen que prestar atención seria a la ciberdelincuencia, la cobertura normativa de



**VOLUNTARIO
AL GILLUM DEL AÑO**

Kevin Anderson, CAMS

Kevin Anderson ha estado con Bank of America desde 1990, trabajando en varias funciones en la banca minorista, seguros y gestión de patrimonios. Desde 1997, ha trabajado en el cumplimiento, centrándose principalmente en temas de antilavado de dinero (ALD). En el cumplimiento, es coautor de los requisitos de la integración de políticas de ALD en toda la empresa y de los programas iniciales de varias empresas, así como las leyes y los reglamentos. Ha participado en las revisiones posteriores, la incorporación de cambios normativos y otros, así como ha proporcionado orientación a las líneas de negocio a nivel mundial. Ha desarrollado y llevado a cabo capacitación en ALD y evaluaciones de riesgos de la empresa, así como al nivel de la unidad de negocio. Diseñó, implementó y logró el proceso de la empresa para obtener y validar las certificaciones de la Ley del Patriota para bancos no estadounidenses durante varios años. Ha construido e implementado procesos para apoyar la documentación continuada de la política y el programa de ALD.

Además de la labor de política de ALD, Anderson ayudó a diseñar y establecer un marco para supervisar el desarrollo y aplicación del cumplimiento en toda la empresa y las políticas de riesgo operacional, incluyendo la privacidad, el préstamo razonable y los riesgos de los sistemas de pago.

Anderson ha sido Especialista Certificado en Antilavado de Dinero (CAMS) desde 2003 y ha sido miembro del Grupo de Trabajo Editorial y Grupos de Tareas de Educación de ACAMS durante varios años. Ha publicado numerosos artículos sobre temas de lavado de dinero en revistas como *ACAMS Today* y la *ABA Banking Journal*.



PREMIO PIONEER DE ALD

Michael R. McDonald, CAMS

Michael R. McDonald es veterano del Servicio de Impuestos Internos (IRS), División de Investigación Delictiva, con 27 años de experiencia. Se jubiló en 1998 y formó una consultoría con sede en Miami especializada en el lavado de dinero internacional, la Ley de Secreto Bancario (BSA), la Ley del Patriota, la confiscación de bienes, el cumplimiento y asuntos relacionados. La empresa es una red de agentes especiales jubilados, cada uno con una profunda experiencia en investigaciones de lavado de dinero. Durante su paso por la División de Investigación Criminal del IRS, McDonald ejerció varios cargos de agente de campo y de gestión y dirigió los recursos de investigación en muchos grupos de trabajo de lavado de dinero de alto perfil. Fue el gestor principal del desarrollo de la primera fuerza de tareas de lavado de dinero, la Operación Greenback. Fue el primer coordinador del IRS para el Grupo de Tareas de Ejecución del Narcodelito Organizado de Florida/el Caribe y el Grupo de Tareas del área de Florida del Sur de Tráfico de Alta Intensidad de la Droga (HIDTA). Se hizo conocer ampliamente como uno de los expertos de primer nivel del gobierno en materia de blanqueo de dinero y la BSA.



**PROFESIONAL DEL
AÑO DE ALD**

Chuck Taylor, CAMS

Charles "Chuck" Taylor es vicepresidente senior y oficial de la Ley de Secreto Bancario (BSA) del City National Bank (CNB), banco de 30 mil millones de dólares con sede en Los Ángeles, y oficinas en California, Nevada, Nueva York, Georgia y Tennessee. Tiene la responsabilidad de supervisar todos los aspectos de BSA, incluyendo el mantenimiento del programa BSA del banco, la evaluación de riesgos de BSA, el monitoreo del ALD, y la presentación de informes de moneda y actividades sospechosas, el programa de identificación de clientes, filtración de sanciones y capacitación en BSA.

Taylor completó su doctorado en derecho en 2001, recibió su Certificado como Especialista en Antilavado de Dinero (CAMS) en 2003 con la clase inaugural y se convirtió en un Oficial Certificado de BSA en 2007. En 2010, Taylor completó el programa de Gestión Bancaria y Finanzas al nivel de Maestría de la Pacific Coast Banking School. Taylor es miembro fundador y copresidente actual del Capítulo de ACAMS del Sur de California. Taylor es también profesor del Programa de Certificación Avanzada de ACAMS y del Curso Preparatorio para el Examen CAMS.



Nada sustituye la experiencia de primera mano

nuevos métodos para promover valor, y que van más allá de las transacciones financieras tradicionales.

SP: La amenaza terrorista es el desafío mayor y tenemos que mejorar nuestros modos de comunicación y la velocidad a la que somos capaces de transmitir información pertinente.

CS: Creo que la mayoría de las personas en la industria estarán de acuerdo en que las amenazas de ciberseguridad y cibernéticas seguirán planteando un reto aún mayor el año que viene. Una encuesta de CDW Financial Services indicó que el 49 por ciento de las entidades participantes tuvo un ataque cibernético en los últimos 12 meses. La comunidad de ALD/delitos financieros puede cumplir con este desafío con medidas de seguridad proactivas que incluyen:

- Un plan de ciberseguridad sólido
- Recursos adecuados formados en seguridad cibernética
- Infraestructura de IT y tecnología
- Formación y sensibilización mayor sobre la seguridad
- Cumplimiento de las regulaciones de la industria
- Comunicaciones mejoradas con clientes

CT: Las transacciones electrónicas están evolucionando muy rápidamente y requerirán mucha atención en el próximo año. Las monedas virtuales, Apple Pay, ACH del mismo día, transacciones P2P y nuevas formas de procesamiento de pagos plantean diferentes riesgos y beneficios. Adelantarse a todos ellos, tratando de estar debidamente educado, evaluar su riesgo de ALD y poner los controles adecuados es tarea de enormes proporciones. Para mí, personalmente, se trata de lograr que lo que se dice sobre la moneda virtual progrese y conseguir que los bancos se involucren más. Soy un hinchista de la tecnología y espero que pueda adoptarse de manera generalizada en algún nivel. Para prepararse, lo mejor es sumergirse. Si se trata de la moneda virtual que desconcierta más, comprar un poco, utilizarla e ir a una conferencia o reunión lugareña de seguimiento sobre el tema. Nada sustituye la experiencia de primera mano. Sin ella usted no puede tomar decisiones informadas.

AT: ¿Cuál es la lección más importante que ha aprendido?

KA: Sentirse orgulloso de su propio trabajo y que el trabajo de uno refleje el hecho de que uno ha hecho un buen esfuerzo. Los otros lo juzgan a uno no en lo que uno piensa, sino más bien por la forma en que a uno lo perciben. Por lo tanto, el trabajo debe reflejar el hecho de que uno se preocupa. Si usted simplemente envía el trabajo por correo, la gente va a ver eso y reducir la percepción de uno a eso.

BA: Nunca piense ni por un minuto que uno lo sabe todo sobre el ALD. Las técnicas, instrumentos y canales de distribución utilizados por los delincuentes, lavadores de dinero y los potenciales financistas del terrorismo cambian más rápidamente que las leyes y reglamentos, y el profesional de ALD debe operar con la mayor eficacia posible, cerrando las brechas entre los delincuentes y las leyes. Es crucial permanecer centrado, estar al día, aprender a adaptarse a las circunstancias siempre cambiantes y, en última instancia, pensar como un delincuente o lavador con el fin de posicionarse mejor uno mismo para identificar eficazmente las tendencias y amenazas de lavado de dinero si se quiere tener alguna oportunidad en forma efectiva en la lucha contra el problema.

CB: El valor de su red. Esta industria es muy grande y conseguir a quien uno necesita no es siempre fácil ni rápido. Una vez que tenga una tarjeta de visita o incluso un nombre, puede conseguir las respuestas que está buscando en una fracción del tiempo. Es similar a una lección que me enseñaron en la escuela de inteligencia militar: "Usted no tiene que saber todo, sólo hay que saber dónde encontrarlo".

ÉL: Se trata de una cultura de cumplimiento y la cultura necesita tiempo para cambiar.

MM: El lavado de dinero y otros delitos financieros nunca desaparecerán y nunca se podrán detener. Sólo cambiarán el aspecto y la metodología. Todo lo que puede hacer el especialista en delito financiero es mantenerse al día con estos eventos y perseguir al delincuente financiero y sus activos y aumentar la relación riesgo/recompensa a un nivel más aceptable (desde un punto de vista de la ejecución).

SP: Nada es perfecto y hay que seguir trabajando en ello. El ALD es una industria bastante joven y hay muchas cosas que necesitan mejorarse.

CS: Llevar a cabo su negocio con integridad y el éxito seguirá.

CT: Que necesito ayuda. Las decisiones de riesgo se hacen mejor con un montón de entradas y opiniones. El grupo de colegas que tengo aquí en City National se encuentran increíblemente bien informado, experimentado y dispuesto a ayudar. Ellos siempre vienen con ideas y temas que todavía no había considerado.

AT: La motivación es importante para el éxito; ¿puede compartir lo que te motiva?

KA: Los éxitos compartidos me motivan. Siempre he disfrutado de ser parte de un equipo que trabaja bien conjuntamente para desarrollar una solución a un problema, por grande o pequeño que sea. He tenido la suerte en mi carrera de haber trabajado con tantos grandes compañeros de equipo para desarrollar una mejor manera de hacer las cosas. Son los sentimientos de logro y la camaradería y el conocimiento de que podemos tener éxito mediante el trabajo conjunto, que me mantiene motivado para continuar.

BA: Mi motivación viene del deseo de buscar el conocimiento a través de una amplia gama de áreas con el fin de alcanzar y mantener el más alto grado de conocimiento que me sea posible, independientemente de aquello en que centro mi atención. Dentro de la profesión de ALD, esto significa que busco continuamente el conocimiento de funciones cruzadas con la esperanza de que finalmente pueda aprender lo suficiente para enseñar con eficacia y beneficiar a otros.

CB: Hay gente muy mala en este mundo que hace cosas muy malas, pero necesitan recursos para hacerlas. Espero que mi trabajo (nuestro trabajo) les haga más difícil operar y, en algunos casos, les impide hacer más daño.

ÉL: El ALD es muy práctico y, como instituciones financieras, podemos hacer una diferencia.

MM: He pasado más de 45 años en la arena del delito financiero/ALD/financiación del terrorismo. Ganar un juicio me motiva. Me motiva ver los activos procedentes de actividades delictivas ejecutadas y devueltos los ingresos de fraude a las partes perjudicadas. Ver que las transacciones financieras acaban en procesamiento me motiva.



CAPÍTULO DEL AÑO

Éric Lachapelle, M.Sc., CFA, CPA, CGA, CRCP

Éric Lachapelle es director senior de Cumplimiento Corporativo y Antilavado de Dinero del Grupo Desjardins desde 2011. Lachapelle gestiona, entre otras cosas, el Centro de Excelencia responsable del programa de cumplimiento, las relaciones con las autoridades reguladoras y todas las actividades relativas a la prevención y detección de lavado de dinero y la financiación del terrorismo de Desjardins Group.

Antes de entrar a Desjardins Group, Lachapelle ocupó diversos cargos dentro de la industria de servicios financieros, incluidos los de director de servicios de asesoramiento, riesgo, rendimiento, tecnología y cumplimiento de KPMG Canadá, director de riesgos de mercado de Desjardins Securities y asesor independiente para los bancos, fideicomisos, fondos de pensiones y empresas de seguros.

Lachapelle tiene una maestría en finanzas de la Universidad de Sherbrooke. Obtuvo el certificado de Chartered Financial Analyst (CFA) en 2006; el de General Accountant (CGA-CPA) en 2008 y, más recientemente, en 2012, el de Regulatory Compliance Professional (CRCP) de la Wharton Business School.



CAPÍTULO DEL AÑO

Sylvain Perreault, CAMS

Sylvain Perreault es director de cumplimiento de Desjardins Group desde marzo de 2011. Antes de este reciente nombramiento, fue director de operaciones de Desjardins Securities. Trabaja en Desjardins desde 2004.

Perreault es presidente de la junta directiva de la Asociación de Inversión de la Industria de Canadá (IIAC), presidente del Capítulo de ACAMS de Montreal y miembro del Comité de Reglamentación Especial de la Bolsa de Montreal. Es expresidente del Consejo del Distrito de Quebec de la Organización Reguladora de la Industria de Inversiones de Canadá (IIROC), expresidente de cumplimiento y de la Sección Legal (CLS) de IIROC así como expresidente del Comité Consultivo Nacional (NAC).

Es miembro de la Asociación de Abogados de Québec desde 1984 y, entre 1988 y 1997, desempeñó diversas funciones en la Bolsa de Montreal, una de las cuales fue la de vicepresidente senior de mercados. Fue también director, mercados de capitales, en PricewaterhouseCoopers, donde dirigió, entre otras cosas, la puesta en marcha de los mercados en los mercados emergentes. Perreault fue uno de los fundadores de Jitney Group, una firma de corretaje especializada en procomercio, donde ocupó la presidencia hasta 2004.

SP: Los jóvenes que entran al campo del ALD—una carrera emocionante los espera.

CS: Cada día presenta retos nuevos y diferentes. Mientras más difícil y desafiante la tarea, más motivada estoy para hacer un buen trabajo y lograr que se haga a la satisfacción de nuestros clientes. Sabiendo que el trabajo duro de uno se valora es un gran motivador.

CT: Asegurar que me las arreglo adecuadamente con el riesgo regulatorio, sin ser un obstáculo para los negocios. Es una línea muy fina que puede ser difícil de manejar, pero siempre es interesante.

AT: ¿Cuál es su momento de mayor orgullo como profesional de ALD?

KA: Creo que probablemente habrá sido el momento en que mi primer artículo se publicó en *ACAMS Today* (en 2007). No había escrito nada para un público amplio desde la escuela secundaria, y ciertamente nada que se distribuyera tan ampliamente como *ACAMS Today*. Recuerdo que le pedí al personal editorial de ACAMS copias adicionales para enviar a amigos y familiares. No me daba cuenta de que sería el inicio de una racha de decenas de artículos para *ACAMS Today*.

BA: Creo que como co-receptor del premio anual de este año del artículo de *ACAMS Today*, si me retirara de la profesión mañana, este sería uno de mis mayores logros. No es por recibir el premio en sí, aunque eso es realmente sorprendente dada las probabilidades, pero a sabiendas de que los líderes y compañeros en mi profesión elegida creían que el artículo del que fui coautor podría potencialmente beneficiar a lo que ahora es una comunidad muy global de ALD. Cuando escribo artículos para *ACAMS Today*, lo hago con la esperanza de que los profesionales de ALD podrían potencialmente ganar la penetración de la información proporcionada.

CB: Después de ser el primero en mi programa en obtener la certificación CAMS, ese logro fue informado en la Oficina del Secretario de Defensa. Resultó un gran éxito para nosotros en el desarrollo del reconocimiento de que los soldados pueden ser valiosos recursos en esta industria compleja.

MM: La creación y el éxito de la Operación Greenback en 1979 en Miami, Florida.

SP y ÉL: El lanzamiento de nuestro Capítulo de Montreal y ayudar a reunir profesionales.

Encuentra lo que te motiva y aquello que te apasiona en esta industria y tendrás éxito

CS: Me siento muy orgullosa cuando me preguntan qué hago para ganarme la vida y puedo explicar el papel de seres humanos y tecnología en la lucha contra la financiación del terrorismo, lavado de dinero y otros delitos financieros. Por supuesto, ser reconocida por mis compañeros y recibir el premio del *Artículo del Año* de ACAMS en Las Vegas este año fue por lejos mi momento más orgulloso hasta ahora.

CT: Tiene que ser recibir este premio basado en el reconocimiento de pares de ALD. Aparte de eso, es cada vez que un colega se toma el tiempo para darme las gracias por ayudar con un tema difícil de BSA. En muchos casos, se sorprenden de que esté dispuesto a explorar las opciones en lugar de decir no al principio.

AT: ¿Algún consejo para los profesionales de ALD que empiezan en el campo de la prevención del delito financiero?

KA: He encontrado que es útil tener un insaciable deseo de aprender cosas nuevas y saborear asumir retos, ya que hace que el trabajo no aburra. Por mucho que un enfoque basado en el riesgo se basa en la interpretación de los hechos, siempre estoy tratando de aprender más sobre el “cómo” y el “por qué” se hacen las cosas, ya que esto pone a los principios subyacentes detrás de un escenario y ayuda a determinar las mejores formas de mitigar los riesgos realmente presentes. La acumulación de este conocimiento y su aplicación en diferentes escenarios en los últimos años me ha hecho algo así como un referente para aconsejar

sobre ALD. Este es el tipo de éxito que hará que un profesional del ALD entre al camino del progreso.

BA: Aconsejaría a cualquier persona nueva en la prevención de delitos financieros que se mantenga en enfocar el aprendizaje continuo. Para obtener cualquier grado de éxito y la longevidad en este campo, las personas deben buscar todas las oportunidades posibles para obtener los conocimientos tanto prácticos acerca de la justicia penal, el fraude, la tecnología de las leyes como los reglamentos e información de ALD y las sinergias entre ellos y estar preparados para aplicar lo que uno sabe en cualquier escenario. Hay una serie de opciones disponibles para las personas con diversos orígenes e intereses.

CB: Encuentra lo que te motiva y aquello que te apasiona en esta industria y tendrás éxito.

MM: Manténgase actualizado y piense fuera de la caja. ¿Recuerda los buscapersonas? No, nadie los recuerda hoy. De eso se trata. Las empresas de buscapersonas nunca imaginaron la explosión de otras tecnologías de comunicación. Lo mismo se aplica al ALD y los delitos financieros. El mundo virtual está aquí para quedarse e incluye la banca móvil, los sistemas de transferencia de valores informales y la falta de cobertura regulatoria adecuada. Así es como el producto del delito se moverá en el futuro.

SP y ÉL: Asegúrese de que sus habilidades de IT siempre están actualizadas o al menos manténgase actualizado ya que la prevención del delito es en gran medida un “juego de datos”.

CS: Sí, esto es lo que yo recomiendo:

1. Involúcrese. Únase a un grupo de la industria tal como ACAMS y participe en tantos eventos de conocimiento como pueda. Hable con otras personas de la industria para obtener su punto de vista sobre temas específicos.
2. Manténgase al día con las tendencias y regulaciones. Lea, lea y lea. Hay un montón de buenos artículos, documentos técnicos y publicaciones.
3. Encuentre un mentor, alguien que se tome el tiempo para hablar con usted y le ofrezca asesoramiento sobre su progresión profesional.
4. Sea una persona emprendedora. Aprenda y haga bien su trabajo, entonces demuestre su voluntad de asumir otras tareas.

CT: Infórmese y relaciónese con la gente que ya están en el campo. Es difícil ingresar sin experiencia por lo que mientras mejor usted pueda discutir con conocimiento de asuntos, más fácil será el progreso en el campo. También tendrá que dejar su ego fuera del juego. Lo más probable es que tenga que empezar desde abajo del tótem, así que no rechace un trabajo de nivel de entrada, porque siente que está por debajo de su nivel. Entre y saque lo mejor que pueda. No pasará mucho tiempo antes de que sobresalga si tiene la actitud correcta y ética laboral.

AT: Me gustaría hacerles dos preguntas específicas adicionales sobre capítulos a Sylvain y Éric. Describan su actividad de capítulo más exitosa y por qué fue tan exitosa.

SP: Todos los eventos de “almuerce y aprenda” fueron grandes éxitos. ¡Los socios están siempre ansiosos por aprender más!

AT: ¿Cómo se puede aumentar la participación en los capítulos?

ÉL: Tener un evento nacional con profesionales reconocidos para que hablen en eventos del capítulo en el futuro cercano.

SP: Más eventos de cóctel. ¡La gente tiene sed y les encanta establecer contactos! **TA**

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

Evaluación del

Estado Islámico

y de grupos terroristas afines
desde una perspectiva del ALD

¿Cómo deberían ver al Estado Islámico los oficiales de cumplimiento de instituciones financieras, los analistas y los investigadores? Por un lado, como ciudadanos preocupados, deberían ver el Estado Islámico como la organización terrorista bárbara y matona que es. Por otra parte, como profesionales de cumplimiento, deben ver la organización como un posible cliente corporativo y los miembros de la organización como posibles clientes individuales. La pregunta entonces es: ¿Cómo identifican los profesionales de cumplimiento a los clientes de la organización e/o individuos como miembros o partidarios del Estado Islámico y de otras organizaciones terroristas?

Una cosa es cierta sobre los profesionales de cumplimiento: son dedicados y apasionados por lo que hacen. Al ver las atrocidades causadas por el Estado Islámico, y a medida que el peligro para los EE.UU. y sus aliados occidentales se hace más pronunciado, los profesionales de cumplimiento quieren saber qué pueden hacer para disminuir la amenaza. El hecho es que hay mucho que pueden hacer. Después de todo, la información financiera es una de las principales vulnerabilidades de los terroristas. El punto de partida para los profesionales de cumplimiento es conocer a su cliente y la identificación de los riesgos asociados a la financiación del terrorismo. En este caso, consiste en saber más sobre el Estado Islámico y sus miembros así como saber más acerca de los grupos terroristas afines y sus miembros que operan en Irak, Siria y la región circundante.

A mediados de 2014, fuentes de inteligencia estimaron que el ISIL tenía activos por valor de \$2 mil millones

Así que, ¿quién es el Estado Islámico y los grupos afines que suponen una amenaza para Occidente?

El Estado Islámico evolucionó a partir de al-Qaeda en Irak (AQI). El precursor de AQI era un grupo llamado Jama'at al-Tawhid wal-Jihad. Fue formado en 1999, por Abu Musab al-Zarqawi. El grupo se trasladó a Irak en 2003 para luchar contra las fuerzas estadounidenses, a raíz de la invasión de Irak. En octubre de 2004, al-Zarqawi oficialmente juró lealtad a la red al-Qaeda de Osama bin Laden. Durante ese período, al-Zarqawi llegó a convertirse en uno de los terroristas más buscados en el mundo debido a sus brutales tácticas. Fue asesinado en un ataque aéreo estadounidense el 7 de junio del 2006. En octubre de 2006, AQI se fusionó con otras cuatro facciones insurgentes y cambió su nombre por el de Estado Islámico de Irak (ISI por sus siglas en inglés). En 2008, el ISI había sido diezmado por el ejército de los EE.UU. Aunque gravemente disminuido, el ISI mantuvo una sólida infraestructura, incluyendo un flujo constante de financiamiento. Abu Bakr al-Baghdadi fue nombrado líder del ISI el 16 de mayo del 2010. Al-Baghdadi repuso el liderazgo y las filas de ISI mediante la contratación de ex oficiales militares y de inteligencia baazistas que habían servido durante el régimen de Saddam Hussein. Estos individuos eran combatientes suníes experimentados. Tras el derrocamiento de Hussein, los EE.UU. disolvió el ejército iraquí y luego ayudó a los iraquíes a establecer un ejército nuevo, que era predominantemente chií. A raíz de la retirada estadounidense de Irak, en julio de 2012, al-Baghdadi, anunció que el ISI estaba regresando a sus antiguos bastiones en Irak.

En agosto de 2011, al-Baghdadi comenzó a enviar combatientes sirios e iraquíes con experiencia ISI a Siria para establecer un grupo allí. Al-Baghdadi nombró a un sirio, Abu Muhammad al-Jawlani, para estar a cargo. Quería que el grupo reclutara combatientes y estableciera células por toda Siria. Al grupo se le llamó el Frente al-Nusra y creció rápidamente. La inestabilidad y el caos en Siria e Irak proporcionaron al ISI y al Frente al-Nusra la oportunidad de prosperar y acumular grandes riquezas. En abril de 2013, al-Baghdadi, anunció que el Frente al-Nusra se había creado, financiado y apoyado por el ISI y que los dos grupos se fusionaban bajo el nombre de "Estado Islámico de Irak y al-Sham" (ISIS por sus siglas en inglés). El Frente al-Nusra no aceptó la fusión y pidió al líder de al-Qaeda, Ayman al-Zawahiri, que intercediera. Al-Zawahiri se pronunció a favor del Frente al-Nusra y le instruyó a ISIS que regresara a Irak. ISIS se negó y continuó operando en Siria, así como en Irak. En consecuencia, ISIS fue desautorizado por al-Qaeda en febrero de 2014. A ISIS también se le conoce como el Estado Islámico de Irak y el Levante (ISIL, según sus siglas en inglés). ISIL es el acrónimo utilizado por el gobierno de los EE.UU. cuando se habla del grupo. El significado del término "Levante" cubre Irak, Siria, Líbano, Jordania, Israel, Palestina, Chipre y parte del sur de Turquía. Los EE.UU. entienden que ISIL aspira a extender su presencia y control más allá de Siria e Irak en cada uno de estos otros territorios.

Si bien el Frente al-Nusra se ha unido con otros grupos rebeldes en Siria y se centró en la lucha contra el gobierno sirio, el ISIL estaba más centrado en ganar control sobre tanto territorio como sea posible en Siria e Irak. Tomaron el control de la frontera con Siria y el territorio iraquí, lo que les daba mayor flexibilidad para mover sus combatientes entre los dos países. El 29 de junio del 2014, el ISIL retiró "Irak y el Levante" de su nombre y ahora se refiere a sí mismo como el "Estado Islámico". Al anunciar el cambio de nombre para el Estado Islámico, el grupo informó que había establecido un califato en el vasto territorio que controla en Siria e Irak. El Estado Islámico convocó a los musulmanes de todo el mundo a jurar lealtad al califa, Abu-Bakr al-Baghdadi, líder del ISIL. El ISIL ha sido ampliamente criticado por la comunidad musulmana por sus acciones.

El Estado Islámico o ISIL ha llamado la atención de los medios de comunicación todos los días desde junio de 2014, y actualmente es el grupo terrorista más reconocible y visible en el mundo. Su sentido profundamente arraigado de propósito y su política, capacidad financiera

y militar han transformado el ISIL en una grave amenaza regional y global. Ha acumulado una riqueza increíble y se ha convertido en el grupo terrorista más rico del mundo. La fuente ilimitada de fondos disponibles para el ISIL le ha permitido crecer, ganar poder y fuerza militar y aumentar su nivel de amenaza.

El ISIL disfruta de múltiples flujos de financiación. Se ha apoderado de los pozos de petróleo en Siria e Irak en los territorios que controla. También impone impuestos y extorsiona a los residentes del territorio bajo su control, sobre todo en Mosul, Irak. Otras fuentes de financiamiento incluyen el pago de rescates de secuestro, robo y venta de antigüedades, saqueo y robos de bancos. En un grado mucho menor, estas fuentes derivan de donantes ricos. Son autosostenibles y, por tanto, no se responsabilizan ante cualquier benefactor. A mediados de 2014, fuentes de inteligencia estimaron que el ISIL tenía activos por valor de \$2 mil millones.

El ISIL es extremadamente sofisticado y tiene un sistema de mando y control efectivo. Además de al-Baghdadi, el ISIL tiene una estructura de liderazgo definido y sentido de organización. Mantiene los comités que supervisan las finanzas, liderazgo, asuntos militares, asuntos legales, asistencia a los combatientes extranjeros, seguridad, inteligencia y medios de comunicación. El ISIL tiene equipamiento amplio, gran parte de lo que ganó en victorias contra las fuerzas militares iraquíes y sirias. El ISIL también tiene soldados profesionales, muchos de los cuales antes estaban en el ejército iraquí bajo Saddam Hussein, como se señaló anteriormente.

El ISIL tiene entre 20.000 y 30.000 combatientes. Aproximadamente 12.000 de estos combatientes son personas forasteras a Siria e Irak. Se estima que 2.000 combatientes extranjeros provienen de Europa, mientras que hasta 200 provienen de los EE.UU. Muchos de los combatientes extranjeros de Europa y de los EE.UU. se han descrito como inadaptados en sus países de origen y más fanáticos que otros combatientes. Ha sido fácil para que los combatientes extranjeros lleguen a Siria a través de Turquía, en particular, y por otros países vecinos. Siria se ha convertido en el lugar preeminente para al-Qaeda y el ISIL para reclutar, entrenar y equipar a un número cada vez mayor de extremistas de países extranjeros.

Además del ISIL, el Frente al-Nusra y otros grupos insurgentes en Siria también han atraído a muchos combatientes extranjeros. La mayoría de los combatientes extranjeros son musulmanes suníes, que vinieron a

luchar contra el régimen de Assad en Siria o el gobierno chií en Irak. A raíz de los ataques aéreos de los EE.UU. contra objetivos terroristas en Siria el 23 de septiembre del 2014, el gobierno de los EE.UU. anunció que uno de los objetivos de bombardeo era un grupo de al-Qaeda conocido como el Grupo de Jorasán. Este grupo está compuesto por combatientes de al-Qaeda experimentados en Pakistán y Afganistán. Fueron enviados a Siria para establecer campos de entrenamiento. Debido al conflicto en Siria, fueron capaces de establecer instalaciones de entrenamiento y operar libremente. Están estrechamente alineados con el Frente al-Nusra. Al anunciar el bombardeo, el gobierno de los EE.UU. declaró que el Grupo de Jorasán representa una amenaza más inmediata a los EE.UU. que el ISIL. El Grupo de Jorasán ha estado trabajando con al-Qaeda en la Península Arábiga (AQPA), el grupo de al-Qaeda con sede en Yemen, para fabricar bombas que podrían pasar por la seguridad aeroportuaria sin ser detectadas. AQAP tiene como fabricante de bombas de al-Qaeda, a Ibrahim al-Asiri, como miembro valioso. Se cree que el Grupo de Jorasán estaba reclutando y entrenando a combatientes extranjeros. La intención era que los combatientes extranjeros regresarían a sus países y cometerían actos de terrorismo. La combinación de la capacidad de fabricación de bombas y combatientes extranjeros que regresaban aumentaba el nivel de amenaza planteada por el Grupo de Jorasán. Los atentados del 23 de septiembre dañaron seriamente las instalaciones de entrenamiento del Grupo Jorasán y resultaron en la muerte de su líder, Muhsin al-Fadhli.

¿Con quién se trata al nivel del miembro del grupo?

Los miembros individuales de estos grupos terroristas incluyen líderes, facilitadores, financieros, administradores y combatientes. En términos de ISIL, los miembros provienen principalmente de Irak y Siria. Otros miembros son combatientes extranjeros, en su mayoría de países de la región. Otros combatientes extranjeros provienen de Europa y los EE.UU. En términos del Frente al-Nusra, la mayoría de los combatientes son de Siria, algunos de Irak y otros son combatientes extranjeros, similar en composición al ISIL. El Grupo de Jorasán se compone de combatientes procedentes de Pakistán y Afganistán, que están en Siria para reclutar y entrenar a combatientes extranjeros. La preocupación alarmante para los países occidentales es que los combatientes extranjeros que viajan con pasaportes europeos o estadounidenses pueden viajar libremente por todo el Occidente. Si esos combatientes regresan a su país de origen o a otros países occidentales, suponen una amenaza significativa para la seguridad. El hecho de que muchos de estos individuos fueran inadaptados en sus países de origen y son muy fanáticos los convierte en una seria amenaza a la seguridad nacional en toda Europa y los EE.UU.

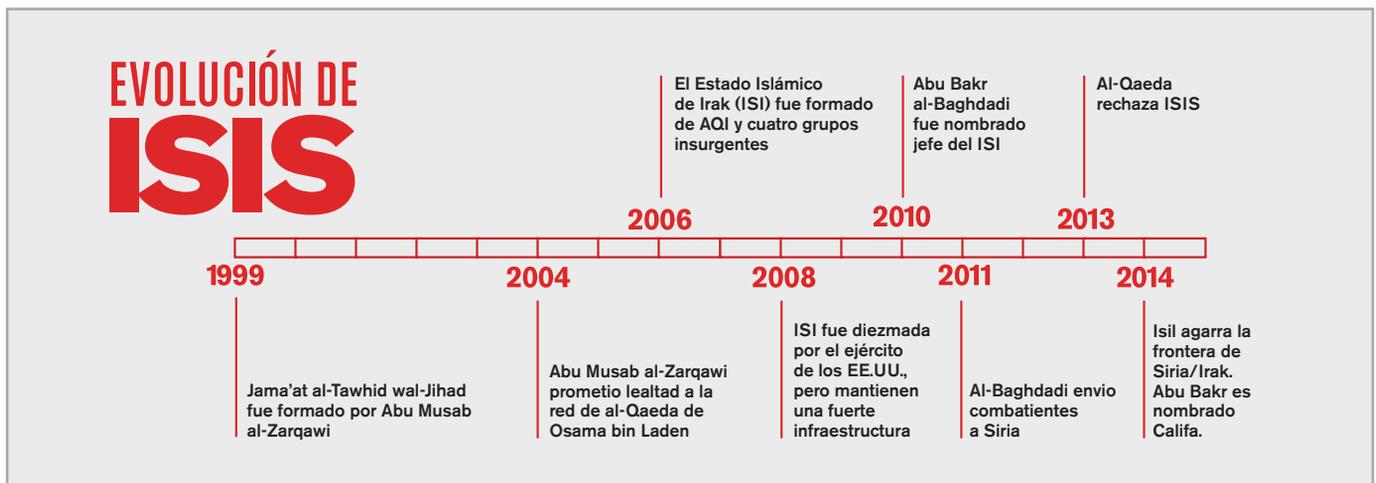
Para reiterar la pregunta formulada al principio de este artículo: ¿Cómo identificar a los clientes profesionales de cumplimiento de la organización e/o individuales como miembros o partidarios del Estado Islámico y otras organizaciones terroristas? Con respecto a la amenaza planteada por ISIL, el Frente al-Nusra, el Grupo de Jorasán y otros grupos similares, los profesionales de cumplimiento deben considerar la amenaza de financiación

del terrorismo en dos niveles: (1) el nivel de la organización y (2), el operativo a nivel del individuo.

Nivel operativo organizacional

En el nivel organizacional, los profesionales de cumplimiento deben evaluar el flujo de fondos en tres tramos. El primer tramo es del dinero que fluye a la organización. En el caso del ISIL, el grupo ha dado lugar a un modelo de negocio con fines de lucro basado en múltiples fuentes de financiación como ya he expresado anteriormente. El segundo tramo es del dinero que fluye de la organización para apoyar las operaciones de la organización. Una vez más, en el caso del ISIL, el dinero de la organización va a fluir a través de la comisión de finanzas, con la aprobación de la dirección. El dinero fluye a través de probabilidades facilitadoras y administradoras para apoyar las operaciones, tales como la financiación de la actividad militar o el costo de la provisión de agua, el pan y la electricidad a los habitantes de los territorios que controla el ISIL. El tercer tramo es la financiación que probablemente se deriva de la comisión financiera a través de los facilitadores y administradores a los combatientes y otros miembros de la organización. Una vez más, en el caso del ISIL podría ser el dinero pagado a los combatientes en la forma de salarios y otras remuneraciones o para otros gastos incurridos en apoyo de la ejecución de sus deberes individuales.

La identificación de la financiación del terrorismo en relación con el ISIL u otros grupos terroristas a nivel de organización es muy difícil. El grupo no estará haciendo operaciones bancarias abiertamente al nombre de ISIL u otros nombres identificables con la organización. Lo más probable es que dependa de



testaferros o empresas fantasmas y de terceros para evitar la detección. La posibilidad de que los frentes o ISIL tengan relaciones bancarias directas con los bancos occidentales es extremadamente remota. Algunos bancos occidentales podrían tener relaciones de corresponsalia con bancos de la región que tienen algún tipo de relación bancaria con el ISIL. Por ejemplo, el ISIL está fuertemente comprometido en la venta de petróleo en el mercado negro de Turquía de los pozos de petróleo que controla en Siria e Irak. Aquí es donde los bancos turcos podrían ser susceptibles de facilitar la actividad financiera del ISIL. Bancos de la región en Jordania y el Líbano también podrían ser utilizados para facilitar la actividad bancaria para la financiación de ISIL como para el petróleo y otras fuentes de financiación. Lugares como Qatar, Kuwait y Dubai, amigables al dinero en efectivo, podrían ofrecer atractivas y seguras oportunidades bancarias del ISIL también. Lo mismo es probablemente cierto con ciertas ubicaciones de banca offshore. Debido a la naturaleza de economías que trabajan en efectivo en Siria e Irak, una gran cantidad de actividad financiera se llevará a cabo en las transacciones en efectivo, lo que sería prácticamente imposible de identificar o controlar por los bancos occidentales. Otra variable es la posibilidad de utilizar la moneda virtual para convertir y transferir el dinero.

La comprensión de la naturaleza y complejidad del riesgo geográfico en la región es esencial para las instituciones financieras occidentales. Además, la comprensión del riesgo empresarial regional es importante. ¿Envían las transferencias bancarias a y de la región, y es razonable lo que comportan para la actividad empresarial? Debido a la devastación de la infraestructura y el enorme número de refugiados en Irak y Siria, hay una enorme necesidad de ayuda humanitaria. Numerosas organizaciones no gubernamentales (ONG) y organizaciones de caridad se encuentran activas en toda la región ofreciendo la ayuda humanitaria que tanto necesitan. Por desgracia, los grupos terroristas de la región toman fondos considerables de las ONG y organizaciones de caridad para apoyar a sus organizaciones terroristas. La actividad caritativa de la región, especialmente en Siria, debe considerarse como un reto y una bandera roja sensible que requiere diligencia debida mejorada (EDD).

Nivel operativo individual

La identificación de las señales de advertencia para la financiación de los miembros individuales del ISIL y otros grupos terroristas en la región debe ser menos difícil que

la identificación de las señales de advertencia de la organización. No obstante, la identificación de las señales de alerta individuales es un reto. Los miembros de grupo individuales procedentes de Irak, Siria y los países no occidentales son mucho menos propensos a tener un nexo con los bancos occidentales. Muchos estarán sin bancarizar. A menos que reciban y gasten fondos de los titulares de cuentas en los bancos occidentales en forma de transferencias electrónicas o actividad ATM, es poco probable que estos individuos estén comprometidos con los bancos occidentales. Por el contrario, estas personas estarían más inclinadas a comprometerse en transacciones de empresas de servicios monetarios (MSB) y en actividad hawala.

Los combatientes extranjeros procedentes de Europa y los EE.UU. tienen más probabilidades de identificarse con los bancos y/o MSB occidentales. En vista de la grave amenaza que suponen estos individuos, su identificación por los profesionales de cumplimiento debe ser una prioridad fundamental. Las personas que aspiran a ser combatientes extranjeros deben ser controlados para viajar a Siria a través de Turquía y otros puntos de entrada para incluir a Jordania, Líbano e Israel. Los profesionales de cumplimiento deben desarrollar patrones de actividad financiera identificable con los viajes en relación con los servicios financieros que su institución ofrece. Una vez que estas personas llegan a Siria, otras banderas rojas se harán más prominentes. Estas señales de alerta incluyen:

- Inicios de sesión de IP en las zonas de conflicto, como cerca de la frontera con Siria, incluyendo Jordania y el Líbano, pero sobre todo Turquía

La comprensión de la naturaleza y complejidad del riesgo geográfico en la región es esencial para las instituciones financieras occidentales

- Los períodos de latencia de transacciones, que podrían ser el resultado de entrenamiento terrorista o participación en combate
- Retiros de efectivo de ATM en zonas de conflicto
- Transferencias bancarias a las zonas de conflicto
- Publicaciones de redes de comunicación social (muchos combatientes extranjeros occidentales utilizan las redes sociales)

Sea que los profesionales de cumplimiento estén considerando organizaciones o individuos, tienen que desarrollar tipologías de casos para mejorar sus capacidades de detectivos. Deben seguir los casos penales y civiles federales. Considerando documentos como información, los procesos y acuerdos de declaración de culpabilidad, se expondrán hechos que establecen el escenario o el patrón de la actividad. Sobre la base de ese escenario o patrón, se pueden desarrollar tipologías de casos. Otros mecanismos que benefician el proceso de identificación incluyen el monitoreo de transacciones, el monitoreo de transacciones dirigidas, informes de prensa negativos y acciones de aplicación de la ley para incluir las solicitudes y procedimientos legales.

Como se señaló al principio, una cosa es cierta sobre los profesionales de cumplimiento: son dedicados y apasionados por lo que hacen. Sabiendo que pueden hacer una diferencia tangible en la identificación de la financiación del terrorismo es algo que les va a resonar y darles una fuente de orgullo y logro significativo. **TA**

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

TPPP:

La delgada línea entre el riesgo y la eficacia

La inclusión de procesadores de pagos de terceros, o TPPP (por sus siglas en inglés), a la cartera de una institución financiera puede tener un impacto positivo en los ingresos de esa organización. Por el contrario, los TPPP también puede plantear riesgos significativos para el lavado de dinero y otras violaciones de reglamentación si no se gestionan adecuadamente. Las instituciones financieras (IF) están encargadas de encontrar el delicado equilibrio entre el aumento de los ingresos y mitigar el riesgo del antilavado de dinero (ALD). Los TPPP, también, tienen una situación difícil a mano—cómo competir dados los muy diferentes requisitos de las IF para los TPPP. Algunos de los requisitos para los TPPP pueden variar, incluso dentro de la misma cartera de las IF. Esto hace que tanto la competencia como el cumplimiento sean muy difíciles para todas las partes involucradas. Este desafío puede mitigarse, sin embargo, con una fuerte colaboración entre las IF y TPPP. Con el fin de forjar alianzas sólidas, cada socio debe tener entendimientos y objetivos comunes. Esto ayuda a establecer el frente necesario para ayudar a combatir el lavado de dinero conjuntamente.

Para comenzar la conversación sobre cómo las IF y los TPPP pueden cooperar mejor para detectar y prevenir el lavado de dinero y otros delitos financieros, es fundamental contar con una comprensión de la definición de un TPPP.

Los TPPP se definen como “clientes de los bancos que proporcionan servicios de procesamiento de pago a los comerciantes y otras entidades comerciales. Tradicionalmente, los procesadores contratados principalmente con los minoristas que tenían lugares físicos con el fin de procesar las transacciones de los minoristas. Estas transacciones mercantiles incluían principalmente pagos con tarjeta de crédito, también cubrían transacciones de Automated Clearing House (ACH) [Clearing Automatizado], cheques creados de forma remota (RCC),¹ y transacciones de débito y tarjetas prepagas”. Esencialmente, los TPPP, en nombre de una IF, permiten que los comerciantes acepten tarjetas de pago y transacciones de ACH. Si bien esta función puede servir como otra forma de crear servicios que atan a los clientes de tesorería a la IF, sigue habiendo algunas dudas en cuanto a las obligaciones reglamentarias del TPPP. ¿Están obligados a la misma financiación del ALD y del antiterrorismo (CTF) que las IF están obligados a seguir?

Algunos TPPP, pero ciertamente no todos, pueden categorizarse como empresas de servicios monetarios (MSB). El acto de procesamiento de pagos solo, sin embargo, no es suficiente para definir una organización como una MSB. De hecho, en agosto, la Red Contra los Delitos Financieros (FinCEN) publicó una guía que indica específicamente

que una empresa no se consideraría transmisora de dinero basándose únicamente en las actividades de procesamiento de pagos.² El TPPP puede ofrecer servicios auxiliares que dan lugar a su categorización como una MSB, pero el procesamiento de pagos por sí solo no era suficiente para reunir una designación de MSB. Eso significa que algunos TPPP son MSB y están sujetos a las obligaciones de ALD/CTF.

La pregunta que muchas IF hacen para determinar si deben asociarse con un TPPP es si o no los riesgos (no cumplimiento normativo) son mayores que los beneficios potenciales (retención de clientes, aumento de ingresos). Citan la dificultad de manejar la diligencia debida y la supervisión de TPPP. ¿Pueden confiar en que sus socios TPPP van a aplicar el mismo nivel de rigor a sus programas de ALD como las IF están obligadas a aplicar? Incluso, ¿quieren los TPPP aplicar ese rigor? ¿Van a ser buenos socios?

En la mayoría de los casos, los TPPP quieren ser buenos socios, y con frecuencia ya tendrán programas para monitorear transacciones de actividades sospechosas. Como las IF continúan aumentando sus carteras de TPPP, hay una serie de factores por considerar. Estos factores pueden ayudar a los TPPP e las IF a fortalecer sus asociaciones, prevenir los delitos financieros y aumentar su potencial de ingresos.

¹ Bank Secrecy Act Anti-Money Laundering Examination Manual. https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm

² FinCEN (August 27, 2014) FIN-2014-R009 “Subject: Application of Money Services Business Regulations to a Company Acting as an Independent Sales Organization and Payment Processor” http://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R009.html

La diligencia debida es un paso importante en cualquier programa de gestión de riesgos de terceros. Esto es rudimentario en la protección de cualquier organización, pero es especialmente cierto en el mundo de los TPPP. La idea de llevar a cabo la debida diligencia sobre posibles socios TPPP puede parecer bastante básica, pero con un proceso consistente, repetible y defendible para proceder a la instrucción los socios potenciales tendrán varios resultados positivos. En primer lugar, se protegerá a la IF de participar con un socio potencialmente dudoso. Asegurar que un TPPP tiene suficientes medios financieros y apoyo organizativo para ser buen socio, permitirá que la IF tenga confianza en la longevidad de esa asociación, al tiempo que minimiza las preocupaciones sobre el aumento de la responsabilidad regulatoria. En segundo lugar, una revisión robusta del modelo de negocio del socio potencial le permitirá a una IF saber si el modelo de la pareja es realmente una buena opción para los objetivos y la estrategia de la organización financiera global. ¿Tiene el TPPP un mercado target que la IF puede soportar, o es el mercado target un grupo demográfico de alto riesgo con la que la IF se encuentra incómoda? Si ese es el caso, ¿qué tipo de protocolos y procesos existen dentro del TPPP para mitigar ese riesgo percibido?

Tal vez uno de los efectos más importantes de un fuerte proceso de diligencia debida es asegurar un campo de juego parejo en la cartera de TPPP. No es raro escuchar que los comerciantes se resistan a proporcionar información sobre el propietario mayoritario. De hecho, los comerciantes a menudo amenazan con llevar su negocio de procesamiento a otra empresa—a “una que no es tan severa”. En algunos casos, ese TPPP no tan severo puede incluso estar en la misma cartera de IF. Esto no sólo es perjudicial para los ingresos, sino que puede introducir un riesgo significativo a la IF, particularmente a la luz del mayor escrutinio regulatorio a que se enfrenta toda la industria.

El aumento del escrutinio regulatorio se manifiesta más claramente en la Operación Chokepoint (Operación Cuello de Botella), iniciativa del Departamento de Justicia (DOJ) para erradicar la mala conducta en el ámbito mercantil mediante hacer a los TPPP, y por extensión, las IF responsables del mal comportamiento. En concreto, la Operación Cuello de Botella se dirige a ciertos tipos de negocio que el DOJ cree que sirven de apoyo a la conducta comercial “desfavorable”. Esos tipos de negocio incluyen TPPP y organizaciones de ventas independientes (ISO según siglas en inglés). Esto ha tenido un impacto

significativo en los procesadores de pago y los ISO, como la Operación Cuello de Botella se ha traducido en más de 50 citaciones a IF. Huelga decir, la comunidad de IF ha reaccionado imponiendo más restricciones en sus TPPP. De hecho, muchos TPPP actuaron de forma independiente para revisar sus propias prácticas y hacer ajustes, actuando con un exceso de precaución.

Si bien el impacto y la eficacia de la Operación Cuello de Botella es terreno fértil para el debate (de hecho, se ha propuesto legislación para detener la operación), un resultado cierto es que los TPPP reconocen que es poco probable que el mal comportamiento de su parte, o por parte de sus comerciantes patrocinados, permanezca en las sombras. Ha enseñado a muchos procesadores de pagos que tienen que crear procesos coherentes, repetibles y defendibles que rigen la forma en que abordan, monitorean, y si es necesario, finalizan la relación con comerciantes “malos”. El apetito por el riesgo en el sector de los pagos sin duda ha disminuido como consecuencia de ello. Así que, ¿cómo pueden las IF y los TPPP trabajar juntos para combatir el lavado de dinero, el financiamiento del terrorismo y otros delitos financieros? La respuesta breve es, trabajando como socios.

Es cierto que no todos los TPPP son una MSB regulada. Eso significa que cuando se asocia con estas organizaciones, la IF debe tener un programa fuerte para educar a los TPPP en cuanto a qué controles deben existir. Las IF pueden obligar contractualmente a los TPPP al mismo nivel de rigor en sus normas de ALD que deben cumplir las entidades reguladas. Pero la obligación contractual por sí sola no es suficiente para asegurar que el TPPP mantendrá un programa sólido y permanente. Esto es cierto incluso si el TPPP tiene la mejor de las intenciones. El monitoreo continuo puede ayudar a mantener al TPPP en el camino correcto, y mitiga el potencial de que la IF acumule riesgo imprevisto en caso de que las prácticas vigentes en su TPPP fallen.

Un elemento crucial de la asociación con éxito es la educación. No es raro que la IF sea más conocedora de las tendencias delictivas financieras que sus socios TPPP. En la misma línea, la IF puede tener significativamente más penetración en cuanto a los métodos que pueden emplearse para controlar, detectar y prevenir actividades sospechosas con éxito. Por estas razones, la IF debe asumir una especie de papel de “mentor”, con los TPPP nuevos. ¿Cómo puede el TPPP mejorar sus programas y prácticas para cumplir con los estándares

de la IF? ¿Qué tipo de controles deben existir? ¿Qué recursos están disponibles para que el personal de riesgo en el TPPP pueda empezar a reunir información y educación por su cuenta? Recordando que el objetivo es la creación de una asociación, la IF debería alentar, incluso exigir, que el personal de TPPP responsable de transacciones y monitoreo de la actividad participen en seminarios de educación y sensibilización para que sean competentes en los requisitos de la Ley de Secreto Bancario/antilavado de dinero (BSA/ALD). Las mejores asociaciones se producen cuando hay un flujo libre de información entre los socios que están igualmente informados acerca de los problemas que enfrenta la industria.

Ese último punto, el libre flujo de información, trae a la mente el componente quizás más importante de la asociación de BSA/ALD entre la IF y TPPP. Ese componente es la comunicación. Si bien los TPPP deben informar a sus socios de la IF de las tendencias o patrones que están viendo, esa información también debe fluir a otros TPPP en la cartera. Si un proveedor de servicios ve un patrón, entonces es muy probable que otros hayan visto patrones similares. El intercambio de esta información entre los de la cartera TPPP, puede actuar como un “multiplicador de fuerza”. En esencia, la IF puede actuar como coleccionista de información y proveedor de inteligencia, mediante la recopilación de información de TPPP respecto de los patrones de comportamiento sospechoso y métodos eficaces para detectar y evitar ese comportamiento. Esta práctica podría ayudar a frustrar los intentos de colocar y mover fondos obtenidos ilícitamente.

La adición de una cartera de TPPP seguramente puede introducir nuevos riesgos. Si se gestiona correctamente, sin embargo, puede no sólo que aumente los ingresos sino que puede aumentar la capacidad de detectar y prevenir el comportamiento sospechoso. La línea entre una propuesta arriesgada y una asociación eficaz es la gestión adecuada. Tan simple como suena, encontrar el equilibrio adecuado puede ser un asunto complicado. La coherencia y la comunicación entre los que participan en la cartera de TPPP pueden ayudar a agregar al crecimiento de los ingresos, a la vez que al mantenimiento de una estrategia responsable de ALD. 

Heather Mark, Ph.D., CAMS, CCEP, SVP, cumplimiento, ProPay, Lehi, UT, EE.UU., heather.mark@propay.com

LA FINANCIACIÓN DEL TERRORISMO:

EL ATENTADO DE MUMBAI, UN ESTUDIO DE CASO EN LO

posible Y LO probable



Entre el 26 y 28 de noviembre del 2008, el mundo fue sorprendido por un ataque terrorista muy bien planificado y ejecutado en Mumbai, India. El grupo Lashkar-e-Taiba (LeT), con base en Pakistán, llevó a cabo el ataque. Diez terroristas, desplegados en dos equipos, atacaron cinco sedes desprevenidas con precisión casi simultánea. Mataron a 166 personas e hirieron a otras 308. Hubo un número incalculable de rehenes y de gente escondida dentro de ciertos lugares de ataque. Como resultado del caos, la confusión y la falta de inteligencia adecuada, durante tres días hubo un agónico empate entre el terrorismo, la actuación policial, la lucha contra el terrorismo y las autoridades militares.

LeT obtuvo un éxito rotundo captando la atención mundial durante el asedio y con sus secuelas. Para cuando las autoridades controlaron la situación, nueve de los 10 terroristas habían muerto, junto con sus víctimas. El décimo operativo LeT fue capturado. El mundo se quedó atónito y país por país miraron a su interior en busca de vulnerabilidades de ataques similares.

Desde Mumbai, ha habido muchas evaluaciones exhaustivas de inteligencia de la violencia y las vulnerabilidades asociadas con ese ataque. Se generaron numerosos informes, de amplio análisis, con fines de inteligencia futuros. Por desgracia, hay poca referencia a la inteligencia financiera. ¡Qué pena!

Dos de las vulnerabilidades más importantes de las organizaciones terroristas, agentes terroristas y operaciones terroristas son las finanzas y las comunicaciones. Una evaluación de inteligencia financiera de Mumbai habría arrojado valiosa inteligencia financiera para la comunidad de inteligencia, aplicación de la ley y, lo más importante, para las instituciones financieras. Sí, las instituciones financieras. Lo que la comunidad de aplicación de la inteligencia y la ley debe recordar cada vez que hay un 9/11 o un Mumbai es que las instituciones financieras son los depositarios de la inteligencia financiera que proporcionará resultados tangibles de investigación antes de muchas otras formas de inteligencia.

Las instituciones financieras y la inteligencia financiera: Lo posible y lo probable

Las instituciones financieras son depositarias de extensa documentación financiera y de apoyo. Esta información es la fuente de inteligencia financiera valiosa. Muchas instituciones financieras han establecido unidades de inteligencia financiera (UIF). Otras han designado personal con responsabilidades de inteligencia financiera. Estas entidades e individuos son responsables de analizar los datos internos y externos para identificar e informar de actividades sospechosas, así como otras vulnerabilidades de riesgo hasta incluir la financiación del terrorismo.

Desde un punto de vista de institución financiera, es posible identificar el financiamiento del terrorismo; sin embargo, no es probable. Dondequiera que podemos identificar lo posible y ampliar a través de análisis de incidentes terroristas como Mumbai, aumentamos la posibilidad de identificar la actividad terrorista más probable. Los elementos del ataque de Mumbai ofrecen modos de comportamiento que, cuando se evalúan en relación con la

inteligencia financiera, aumentan la probabilidad de identificar señales de alerta compatibles con el comportamiento terrorista.

El ciclo de ataque terrorista

Stratfor es un servicio privado prominente y fiable que publica informes de inteligencia, análisis e investigaciones para el gobierno, la industria privada y las instituciones de investigación. En 2005, Stratfor publicó el ciclo de ataque terrorista. Fue lanzado en seis segmentos que identificaron las etapas que los aspirantes a terroristas deben seguir a fin de tener un ataque exitoso. Las seis etapas incluyen:

1. Selección de los blancos
2. Planificación (la financiación es un elemento de planificación)
3. Despliegue
4. Ataque
5. Escape
6. Explotación

El éxito alcanzado por LeT en la realización del ataque de Mumbai demuestra lo bien que siguieron el ciclo de ataque terrorista. A finales de 2005, líderes de LeT designaron a un operativo LeT para que viajara a la India y llevara a cabo vigilancias para identificar blancos para

un ataque para otros operativos de LeT. Una evaluación de la inteligencia financiera relativa a las actividades de este operativo terrorista proporcionaría información valiosa que identifica características operativas compatibles con los agentes terroristas. En la página siguiente, la figura 1 muestra la aplicación de LeT del ciclo de ataque terrorista.

El ataque de Mumbai

Antes del ataque de Mumbai, a LeT se le consideraba un grupo que representaba una amenaza regional. No se le consideró una amenaza para Occidente. Sin embargo, tras el ataque de Mumbai, las agencias de inteligencia determinaron que permiten ataques planificados en Occidente, hasta incluir a los EE.UU. Un ataque estaba en la etapa de planificación. Se dirigía al periódico Morgenavisen Jyllands-Posten en Dinamarca. El ataque iba a ser en represalia por la publicación de caricaturas del profeta Mohammed.

Respecto al ataque de Mumbai, LeT quería matar a la mayor cantidad de occidentales y judíos posible. Esto supuso tomar en cuenta la selección de objetivos. Los blancos elegidos fueron:

- La estación de tren CST
- El Café y Bar Leopold
- El Taj Mahal Hotel
- El Oberoi-Trident Hotel
- Chabad House (Casa Jabad, en español)

Cuando los 10 agentes de LeT desembarcaron en la costa del puerto de Mumbai en la noche del 26 de noviembre del 2008, se dividieron con precisión en cinco grupos y procedieron a sus objetivos asignados.

La estación de tren CST es la sede de Ferrocarriles Centrales y 3,5 millones de personas pasan por la estación diariamente. A las 9:20 de la noche, un equipo LeT entró en la estación de tren CST y comenzó a disparar indiscriminadamente y a tirar granadas. La matanza provocó 58 muertos y 104 heridos. Estos dos agentes habían perdido su teléfono satelital, no parecían utilizar teléfonos celulares y no tenían contacto con el mando y control de la operación de los líderes LeT en Pakistán. En consecuencia, salieron de la estación y robaron un vehículo después de un tiroteo con la policía. Se enfrentaron, en última instancia, con un control policial. Uno de los terroristas fue asesinado y uno capturado.

El Café y Bar Leopold fue inaugurado en 1871. Era un lugar popular frecuentado por extranjeros e indios. A las 9:40 de la noche, un equipo de LeT entró en el Leopold y comenzó



FIGURA 1

Selección del Blanco

Un operativo LeT viajó a Mumbai durante cinco visitas extensas entre mayo de 2006 y julio de 2008. El operativo estableció un frente de negocios como cobertura. Llevó a cabo vigilancias de video extensas de numerosos lugares. En última instancia, cinco lugares fueron elegidos para el ataque. Este operativo también tomó videos de vigilancia extensos del puerto de Mumbai y compró un dispositivo GPS para identificar la ruta que los atacantes tomarían para llegar a Mumbai por agua. Antes y después de cada viaje, el operativo de vigilancia LeT se reunió con líderes de LeT en Pakistán para revisar, evaluar y seleccionar los cinco objetivos.

Planificación

Los ataques fueron meticulosamente planeados por los dirigentes de LeT durante un período de dos años. El operativo de vigilancia estaba bien entrenado y cuidadosamente elegido. La operación fue financiada por un funcionario de la Dirección de Inteligencia Interservicios de Pakistán (ISI). Hubo poca mención de la financiación o el gasto de fondos en los informes de inteligencia sobre el ataque.

Inicialmente, 32 agentes de LeT recibieron entrenamiento con armas de fuego, municiones, granadas y explosivos. Posteriormente fueron entrenados para disparar rifles Kalashnikov, pistolas nueve milímetros y explosivos. Este grupo fue reducido a 13 operativos. Seis fueron escogidos para otras tareas. Tres miembros fueron adicionados. Los 10 agentes de LeT se capacitaron a fondo para llevar a cabo un ataque terrorista. El grupo de 10 hombres fue informado de la operación de Mumbai a mediados de septiembre de 2008. A partir de ese momento, el grupo fue aislado en una casa de seguridad en Karachi, Pakistán y separado de cualquier contacto con el exterior.

Despliegue

Los agentes salieron de la casa de seguridad el 22 de noviembre del 2008. Viajaron en barco a Mumbai. Se transfirieron de un pequeño bote a un barco pesquero indio que otros operativos LeT habían secuestrado. El equipo de ataque dejó el pesquero el 26 de noviembre del 2008, cerca del puerto de Mumbai y viajó a la costa en un bote de goma después de recibir el visto bueno de la dirección LeT en Pakistán. Cada operativo tuvo un amplio suministro de armas de fuego, granadas y bombas. Siguieron cuidadosamente el trazado de la costa previsto con el fin de evitar la detección.

Ataque

Los 10 agentes de LeT irrumpieron en cinco equipos de dos hombres y procedieron a los cinco lugares de destino. Los atacantes estaban bien coordinados y dieron el golpe a cada objetivo de ataque seleccionado en estrecha proximidad temporal. Los ataques fueron una sorpresa táctica e inicialmente encontraron poca resistencia. Muchas de las víctimas que murieron fueron asesinadas en las etapas iniciales del ataque.

Líderes de LeT en Pakistán mantuvieron el mando y control de la operación por teléfono desde Pakistán. Estuvieron en contacto constante con cuatro de los equipos de ataque. El quinto equipo perdió su teléfono satelital al abandonar el barco pesquero. El quinto equipo no parece haber usado teléfonos celulares y no tenía contacto con los dirigentes de LeT en Pakistán. El elemento de mando y control supervisaba la cobertura mediática de cerca y mantuvo a los atacantes informados sobre la posición y los movimientos de la policía india y recursos contra el terrorismo.

Escape

Desde el principio, los 10 atacantes sabían que estaban en una misión suicida. Por lo tanto, no era necesario escapar. Al no estar preocupados por escapar, los agentes de LeT estaban más centrados, destructivos y crueles acerca de sus tareas de ataque.

Explotación

LeT coreografió el ataque para ostentar la atención de los medios con el éxito de la operación. LeT logró la atención de medios globales extendida y cobertura, causando temor en todo el mundo y preocupación por los ataques de estilo similar. Además, LeT tuvo éxito en inflamar las tensiones entre India y Pakistán.

a disparar de manera indiscriminada. Una granada fue lanzada y estalló. Diez personas murieron y muchas resultaron heridas. Los dos atacantes dejaron el Leopold en cuestión de minutos y corrieron hacia el Taj Mahal Hotel.

El Taj Mahal Hotel fue construido en 1903. El hotel tiene 565 habitaciones. Es un icono en Mumbai. Los primeros dos terroristas entraron en el vestíbulo principal del Taj Mahal a las 9:38 de la noche. Abrieron fuego y mataron a 20 personas en cuestión de minutos. El segundo par de terroristas, que venía del Leopold, entró al Taj Mahal a las 9:43 de la noche. Dispararon indiscriminadamente y lanzaron granadas. Los cuatro terroristas fueron a la sexta planta del hotel, matando a todo el que se interponía en su camino. Prendieron fuego a parte del hotel y tomaron rehenes. Además, muchas personas se escondían en sus habitaciones. Los cuatro terroristas mantuvieron contacto telefónico constante con sus líderes en las instalaciones de mando y control en Pakistán. Al final de la disputa, el 28 de noviembre, los cuatro terroristas fueron matados.

El Oberoi-Trident Hotel tenía 877 habitaciones. A las 10 de la noche dos agentes de LeT entraron en el vestíbulo principal del Trident y comenzaron a disparar indiscriminadamente. Cruzaron al Oberoi, matando a los huéspedes y el personal en su camino. Se rociaron balas en un restaurante. Fueron a la planta 16 del Oberoi donde mantuvieron muchos huéspedes como rehenes. Los dos terroristas se mantuvieron en contacto telefónico constante con sus controladores en Pakistán. En la tarde del 28 de noviembre, los dos terroristas murieron.

La Casa Jabad era un edificio de cinco pisos y propiedad de una organización judía ortodoxa llamada Movimiento de Liberación de Jabad de Judíos Jasídicos. A las 10:25 de la noche, dos terroristas empezaron a disparar desde fuera del edificio. Ganaron el acceso al edificio y se llevaron a varias personas como rehenes. Los dos agentes de LeT tuvieron tiroteos con la policía desde el 26 hasta el 27 de noviembre. Estaban en contacto telefónico constante con sus controladores en Pakistán. Los dos terroristas fueron asesinados el 27 de noviembre y cinco rehenes fueron encontrados muertos, asesinados por los terroristas.



**David Coleman Headley:
La conexión de los EE.UU.**

David Coleman Headley nació Daood Sayed Gilani. Nació en Washington, D.C. Su padre era un famoso locutor paquistaní. Su madre era de una familia rica de Filadelfia. La familia se trasladó a Pakistán cuando Headley era bebé. Headley creció en Pakistán. Sus padres se divorciaron y su madre regresó a Filadelfia. Headley se trasladó a vivir con su madre cuando tenía 17 años y viajaba con frecuencia entre los EE.UU. y Pakistán.

Headley se unió al LeT. Asistió a los campos de entrenamiento de LeT en cinco ocasiones entre 2002 y 2003. La formación que Headley recibió incluyó:

Febrero de 2002	Curso de tres semanas	Adoctrinamiento sobre los méritos de librar la yihad
Agosto de 2002	Curso de tres semanas	Formación en el uso de armas y granadas
Abril de 2003	Curso de tres meses	Formación en tácticas de combate y supervivencia
Agosto de 2003	Curso de tres semanas	Formación en contra-vigilancia
Diciembre de 2003	Curso de tres meses	Formación en combate y entrenamiento táctico

En 2005, Headley fue seleccionado por Sajid Mir, un líder de LeT, y el Mayor Iqbal, de la ISI, para viajar a la India para realizar vigilancias de posibles objetivos para un ataque terrorista. La residencia principal de Headley se encuentra en Chicago, Illinois, pero viajaba con frecuencia a Pakistán. En febrero de 2006, Headley cambió su nombre de Daood Gilani a David Coleman Headley. Esto le permitiría presentarse en la India como estadounidense y no como musulmán o paquistaní. En junio de 2006, un viejo amigo de Headley, Tahawwur Hussain Rana, permitió que Headley utilizara su empresa

de inmigración First World Immigration para cubrir las actividades de vigilancia de Headley en Mumbai.

Entre septiembre de 2006 y julio de 2008, Headley hizo cinco viajes prolongados a Mumbai donde llevó a cabo extensas vigilancias de video. Antes y después de cada uno de estos viajes, Headley se reunió con sus controladores de LeT y del ISI de Pakistán en relación con su actividad de vigilancia y selección de objetivos.

Antes de los ataques de Mumbai, a principios de noviembre de 2008, Headley comenzó a realizar vigilancias del periódico Morgenavisen Jyllands-Posten como objetivo en dos localidades en Dinamarca. A principios de agosto de 2009, Headley viajó a Copenhague, Dinamarca para llevar a cabo una vigilancia adicional del periódico. Tomó aproximadamente 13 videos de vigilancia. Regresó a los EE.UU. en o alrededor del 5 de agosto. El 3 de octubre del 2009, Headley fue arrestado por el FBI en el O'Hare Airport de Chicago. Se estaba preparando para viajar a Pakistán para reunirse con Mir y el Mayor Iqbal para proporcionarles los 13 videos de vigilancia.

Headley fue arrestado por sus actividades en relación con el ataque planeado en Dinamarca. Posteriormente, fue vinculado con el ataque de Mumbai. Headley fue acusado por su participación en el ataque de Mumbai y por su participación en el ataque planeado en Dinamarca. Tras su detención, Headley cooperó con el FBI. Proporcionó pruebas en contra de otros conspiradores en ambas tramas. Headley se declaró culpable de los cargos en su contra y atestiguó en contra de otros individuos.



La inteligencia financiera es una poderosa herramienta de investigación

Las lecciones aprendidas por las entidades financieras: Las banderas rojas con respecto a David Headley

Supongamos que por ser un ciudadano de los EE.UU., cuyo domicilio principal era Chicago, Illinois, David Headley frecuentaba uno o más bancos de los EE.UU. Desde la perspectiva de la institución financiera, el ataque de Mumbai ofrece muchos datos de inteligencia financiera. Comienza mucho antes del ataque con la actividad de Headley. Muchas de las banderas rojas identificables con Headley son las mismas banderas identificables con otros agentes terroristas en este caso, al igual que en muchos otros casos de terrorismo.

Comienza en el año 2002. Entre 2002 y 2003, Headley asistió a cinco cursos de formación de LeT en Pakistán. Tres eran de tres semanas de

duración, dos eran de tres meses. Este tipo de entrenamiento es muy intenso. Durante tres, tres períodos de una semana, y dos, períodos de tres meses, Headley habría desaparecido de la red. Probablemente no habría habido actividad bancaria o financiera identificable con Headley durante esos períodos de tiempo. Ese patrón de actividad sería cuestionable en sí mismo. Sin embargo, parejo con los viajes hacia y/o desde Pakistán, un país de alto riesgo para el terrorismo, ese tipo de actividad debe dar lugar a una bandera de alerta de inmediato. Una de las áreas que preocupan a la Sección de Operaciones de Financiación del Terrorismo (TFOS) del FBI es este patrón de actividad. Es una de las banderas más grandes que indican que los individuos están recibiendo entrenamiento terrorista.

La residencia principal de Headley estaba en Chicago, Illinois. En su juventud, vivió en Pakistán. Su padre residía en Pakistán y Headley viajaba a Pakistán con frecuencia. Tener familia en Pakistán justificaría visitas frecuentes. Sin embargo, al evaluar los patrones repetidos de los viajes de los EE.UU. a Pakistán a Mumbai, India, a Pakistán y luego de vuelta a los EE.UU., la sospecha podría haberse planteado. Esto sería especialmente el caso con posterioridad al ataque de Mumbai. LeT, un grupo paquistaní, fue responsable del ataque. Headley viajó con frecuencia entre Pakistán y Mumbai. Añádase el hecho de que se alojó en el Taj Mahal Hotel durante sus viajes de Mumbai. El Taj Mahal Hotel fue uno de los blancos de ataque.

Para la cantidad de viajes realizados por Headley, no tenía trabajo apreciable o fuente de ingresos aparente. Utilizó el negocio First World Immigration Services de su amigo Tahawwur Rana como frente de negocios. ¿Acaso Headley recibió alguna compensación aparente de esa empresa? La inteligencia financiera limitada informada sobre el ataque de Mumbai declaró que Headley fue financiado por el Mayor Iqbal del ISI paquistaní. ¿Mandó el Mayor Iqbal cables a Headley desde Pakistán a los EE.UU.? ¿Se le proporcionó a Headley dinero en efectivo? ¿Cómo obtuvo Headley esta fuente de financiación en su cuenta(s) bancaria? Estas son todas buenas preguntas que podrían haber alertado al (los) banco(s) de Headley.

Durante sus estancias en Pakistán y Mumbai, ¿retiró Headley de cajeros automáticos, especialmente si los fondos estaban siendo depositados en su(s) cuenta(s) bancaria(s) en los EE.UU.? Retiros en cajeros automáticos, en los países de alto riesgo, por parte de ciudadanos estadounidenses son otro punto focal para

TFOS del FBI. Si Headley hizo retiros en cajeros automáticos tanto en Pakistán como Mumbai, secuenciado con sus viajes, esto habría sido una bandera roja significativa.

La cobertura mediática del arresto de Headley, el 18 de octubre del 2009, por proveer apoyo material a terroristas, tendría que haber desencadenado comprobaciones bancarias contra Headley. El (los) banco(s) donde Headley mantiene cuentas tendría(n) que haber alertado y tendría que haberse investigado la actividad transaccional de Headley. Si la actividad anteriormente descrita no lo había marcado previamente, es muy probable que tuviera que hacerse en esta coyuntura.

También es probable que el (los) banco(s) de Headley habría(n) determinado si Headley había realizado actividad de Internet y/o de la banca móvil. Al hacerlo, ¿se identificaron las direcciones IP que Headley podría haber utilizado en Pakistán, como una dirección IP registrada al ISI o identificable como de los miembros conocidos de LeT? De la misma manera, ¿identificarían los bancos los teléfonos celulares o teléfonos satelitales vinculados a Headley que podrían ser rastreados por la policía a la ISI o a LeT? ¿Qué información adicional al proceso de inteligencia financiera del banco habría descubierto? ¿Se habrían centrado en su cambio de nombre? ¿Se habrían centrado en su compra de un dispositivo GPS en Mumbai o la gran cantidad de equipos de video que Headley compraba y utilizaba?

Conclusión

En verdad, al menos un banco de los EE.UU. encontró fragmentos de información de inteligencia financiera, descrito en la parte de arriba, con respecto a David Headley. Es probable que este banco haya proporcionado esa información a TFOS y a otros organismos de investigación.

La inteligencia financiera es una poderosa herramienta de investigación. Desafortunadamente, las más de las veces, se pasa por alto o no se entiende adecuadamente. Cuanto más aprendemos y aplicamos de inteligencia financiera, mayor es la posibilidad y la probabilidad de identificar los David Headley del mundo, que son agentes terroristas extremadamente peligrosos y hábilmente entrenados. **FA**

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

ACAMS® | AML General Awareness

Your Solution for Enterprise-wide AML Training

Annual AML general awareness training for your institution can seem like a frustrating and expensive challenge. ACAMS AML General Awareness will satisfy your competing stakeholders and save you money in the process.

Learn more about this modular e-learning program, featuring “Adaptive Learning,” which adjusts training times based upon the current AML understanding of your staff, potentially saving you and your staff hours of productivity.

ACAMS® 11 of 11 Menu Exit

Money Laundering Basics PREV Slide 3 of 11 NEXT

Money Laundering and Terrorism

While money laundering is related to the proceeds of crime, terrorist financing activities may involve funds that have been raised from perfectly legitimate sources, such as charitable donations.

The recent acts of terrorism throughout the world have increased international efforts to locate and intercept funding for terrorists and their organizations.

Terrorists often control funds from a variety of sources around the world and, in doing so, require the services of skilled professionals, such as those in financial services.

CONTINUE

Visit www2.acams.org/general-awareness for more details

Consejos de FinCEN sobre una cultura de cumplimiento:

**Voz de alerta a
la gestión de la
institución financiera**



Si bien el público normal para los avisos de FinCEN es el personal de cumplimiento, en este caso se está enfatizando a las personas de la institución que tienen la posición más alta que el oficial de cumplimiento del antilavado de dinero (ALD) (y su personal, si la institución es lo suficientemente grande). El aviso señala que les corresponde establecer una cultura adecuada de cumplimiento mediante el establecimiento de un “tono desde lo alto” que se filtra a través de la institución. Los oficiales de cumplimiento de ALD— especialmente aquellos que se enfrentan a los desafíos de obtener los recursos necesarios—deben compartir esto con la alta dirección de su institución para mostrarle que la FinCEN ha incrementado el nivel de responsabilidad individual. Otros reguladores han hablado mucho de considerar a los líderes de alto rango responsables de las fallas de cumplimiento y ahora FinCEN ha dejado constancia con la orientación que se utilizará como clara indicación de que la alta gerencia se encuentra responsable de un programa de ALD efectivo. Cuando las próximas acciones de aplicación surjan (no si, sino cuándo), recuerde usted que uno de los factores para evaluar la penalización es el efecto disuasorio que la penalización tendrá sobre otras violaciones. No es que haya un buen momento para conseguir una acción de cumplimiento, sino que ahora es un momento aún peor.

La guía consolida el déficit que FinCEN ha señalado en recientes acciones de ejecución. Aunque FinCEN señala que las medidas de aplicación son específicas a la institución en particular, muchas de las violaciones derivan de una mala cultura de cumplimiento, que probablemente supongan debilidades en el programa de ALD. FinCEN esboza seis principios clave que ayudarán a fomentar una cultura de cumplimiento en cualquier institución. Aunque la guía se dirige a las instituciones financieras estadounidenses, la orientación contenida puede ser utilizada por cualquier institución en todo el mundo.

1. El liderazgo debe comprometerse

El aviso aclara que el liderazgo incluye el consejo de administración, la gerencia senior y ejecutiva, y los propietarios y operadores— esto se encuentra claramente por encima del nivel del funcionario del ALD. Esto sirve como un reconocimiento de que, si bien el oficial del ALD es responsable de la supervisión del día a día del programa, si el liderazgo no proporciona los recursos necesarios para ejecutar eficazmente el programa, el liderazgo es la parte sobre la cual debe descansar la culpa. Por supuesto, la FinCEN ha tomado medidas

El 11 de agosto del 2014, la Red Contra los Delitos Financieros (FinCEN) emitió FIN-2014-A007, un aviso a las instituciones financieras para promover una cultura de cumplimiento.¹ Este aviso es para ser compartido con la alta dirección de todas las instituciones financieras de los EE.UU. Muchas de las actividades bancarias y de valores reguladores ya han proporcionado orientación sobre las expectativas de cumplimiento aumentados por sus instituciones supervisadas, pero FinCEN la ha extendido a todas las demás instituciones financieras no bancarias y no corredores (non-broker en inglés), incluyendo empresas de servicios monetarios (MSB), casinos y distribuidores de metales preciosos y piedras preciosas.

¹ http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-A007.pdf

en el pasado para hacer frente a los fallos de gestión para proveer un programa eficaz adecuadamente; sin embargo, el asesor debe poner sobre aviso al liderazgo de que fracasos futuros pueden atribuírseles. Ya que FinCEN ha delegado aspectos del programa de supervisión de ALD a otras autoridades que examinan, es importante señalar que, en relación con la multa de la FinCEN contra Pacific National Bank, la Oficina del Contralor de la Moneda (OCC) ejecutó multas contra cuatro miembros de la junta y el CEO.

La advertencia no tiene la intención de asustar al liderazgo, sino más bien animarla. Como el cumplimiento en general es una parte crítica del funcionamiento de una institución exitosa, es importante que el liderazgo entienda que sirve como modelo para el resto de la institución y que debe demostrar un compromiso con el cumplimiento. Este cumplimiento puede ser demostrado de varias maneras, incluyendo las declaraciones de política aprobadas por el liderazgo que se transmite claramente al personal de la institución, como en la formación que requiere el programa. Por supuesto, el liderazgo también tiene que recibir entrenamiento para entender la importancia del cumplimiento y cuáles son las obligaciones de cumplimiento en la institución. Esto, junto con actualizaciones periódicas sobre el estado general de cumplimiento de ALD dentro de la institución, permitirá al liderazgo tomar decisiones informadas sobre la forma de proporcionar los recursos adecuados.

2. Los intereses monetarios no deben comprometer el cumplimiento

Esto no debería ser una sorpresa y la gestión debe expresar que mientras ganar dinero a través de la ejecución de la estrategia de negocio es importante, la rentabilidad por sí sola no debe ser una razón para anular las preocupaciones de cumplimiento válidas. Además, esto incluye la necesidad de proporcionar, en forma permanente, los recursos suficientes para permitir que el programa cumpla con sus obligaciones reglamentarias (por ejemplo, la presentación de informes de transacciones en efectivos [CTR] y los reportes de operaciones sospechosas [ROS]) y mitigar los riesgos de ALD para la institución. También es fundamental que la función de cumplimiento de ALD sea lo suficientemente independiente de la línea de negocio para que sus decisiones no se encuentren excesivamente influenciadas por la línea de negocio. FinCEN ofrece el ejemplo de una MSB con una relación rentable pero preocupante con una agencia. La función del ALD debe ser capaz de llevar a cabo una

investigación independiente e imparcial que evaluará los riesgos que plantea a la institución. La institución debe entonces utilizar esos resultados para determinar el curso de acción apropiado, uno que no debe permitir que la rentabilidad de la relación anule la decisión. Sin embargo, debe tenerse en cuenta que puede haber otras consideraciones válidas que pueden entrar en juego y que permitan que la institución anule la decisión de la función de ALD. El objetivo es que la función del ALD debe ser una consideración y la institución no debe centrarse únicamente en la rentabilidad en oposición al riesgo mitigado incorrectamente.

3. La información debe ser compartida por toda la organización

Como se ha señalado ampliamente en las acciones de Madoff y HSBC, la información puede ser conocida en varias partes de la organización que no comparten de manera efectiva con las partes apropiadas. Aunque sería una tarea hercúlea asegurar que no hay oportunidades para prevenir de forma proactiva las oportunidades perdidas, una institución debe tener procesos en lugar—con el apoyo del liderazgo—para habilitar las conexiones que se harán a través de la institución. Las instituciones a menudo recogen cantidades de información importantes sobre sus clientes. Por ejemplo, la información del cliente se puede recoger a partir de las investigaciones de fraude o citaciones recibidas por el departamento legal que pueden ser muy útiles para determinar si deben llevarse a cabo investigaciones adicionales de actividades sospechosas (y presentación de ROS, en su caso). FinCEN también proporciona ejemplos de los casinos que utilizan el marketing y la información de crédito que pueden ser útiles en la investigación de actividades inusuales, así como la presentación de informes generados por el programa de monitoreo del comercio frecuente de compañías de fondos mutuos u otros esfuerzos.

FinCEN también toma nota de que las diferentes entidades jurídicas dentro de la misma organización (por ejemplo, una compañía tenedora bancaria con un banco y una casa de bolsa o un banco con sucursales y filiales extranjeras) deberían tener en cuenta el intercambio de información. Este tipo de intercambio es un poco más complejo, ya que hay una serie de disposiciones de protección de datos y de confidencialidad de ROS que entran en juego en función de la naturaleza del intercambio propuesto, sobre todo cuando se cruzan las fronteras nacionales y se aplican los diferentes regímenes jurídicos y reglamentarios.

Sin embargo, en muchas jurisdicciones, cierta información puede ser compartida con fines de cumplimiento de la empresa y la gestión de riesgos. FinCEN ha proporcionado orientación sobre esto (curiosamente, esto no se observó en el aviso). No obstante, el desarrollo de un proceso que utiliza estas opciones legales es una vía que puede ser apropiada, pero se debe dar una cuidadosa revisión para asegurar que se lleva a cabo correctamente. Sería irónico que, en aras de mitigar el riesgo de ALD, se hayan creado riesgos de confidencialidad del cliente o de privacidad. Sin embargo, hasta que se tomen más acciones legales, en muchos casos, el intercambio puede ser limitado o forzado a funcionar de una manera menos que ideal.

4. El liderazgo debe proporcionar los recursos humanos y tecnológicos adecuados

Uno de los pilares del programa de ALD es el requisito de tener una persona designada responsable de supervisar el cumplimiento del día a día según la Ley de Secreto Bancario (BSA). Sin embargo, no basta con poner a alguien en la posición; la persona designada debe tener el conocimiento y la autoridad suficientes para administrar el programa. Por otra parte, sobre la base de la evaluación del riesgo y el perfil de riesgo de la institución, debe proporcionar los recursos adecuados de personal de apoyo y tecnología para permitir una gestión eficaz del riesgo. Como se ha señalado en muchas acciones de ejecución, las decisiones de liderazgo impropias han incluido la insuficiencia de recursos, lo que resulta en retrasos significativos de alertas, lo cual conduce a que una actividad inusual no se declare durante largos períodos de tiempo; la revisión de alertas por parte del personal insuficientemente calificado, lo que puede dar como resultado una inadecuada toma de decisiones relacionadas con las alertas; y el ajuste incorrecto de los umbrales de alerta basados en la disponibilidad de personal para trabajar las alertas, que pueden impedir que la actividad inusual se detecte, privando así a la aplicación de ley de acceso a la información potencialmente útil. Además, la FinCEN reconoce los desafíos que se presentan con las revisiones manuales y reconoce que las instituciones pueden necesitar recursos tecnológicos adicionales para hacer frente a las zonas de mayor riesgo—en particular aquellas con un mayor volumen de actividad para automatizar más el proceso de revisión, tales como el seguimiento de la actividad inusual o sospechosa.

5. El programa debe ser eficaz y probado por un tercero independiente y competente

Por supuesto, un programa de ALD debe ser eficaz en la mitigación del riesgo. Como parte de esto, el liderazgo debe estar involucrado en su caso en la eficacia del programa—y en la inversión que la institución ha realizado en el programa. Esto puede hacerse de varias maneras, dependiendo del nivel de la dirección y el perfil de riesgo de la institución. Por ejemplo, el liderazgo podría recibir y examinar los informes periódicos sobre las funciones clave de ALD, como la debida diligencia del cliente (DDC) y los esfuerzos de detectar y reportar actividades sospechosas, las evaluaciones de riesgos y los informes de auditoría.

Muchas de las acciones de cumplimiento han citado el fracaso del escrutinio independiente del programa en detectar otros fallos de cumplimiento. Por lo tanto, así como es fundamental contar con un oficial de ALD calificado con los recursos adecuados, también es vital tener una función de auditoría independiente, calificada e imparcial para evaluar la eficacia del programa. Del mismo modo que la gestión debe garantizar que la función del ALD no está indebidamente influenciada por la línea de negocio, la auditoría independiente debe estar libre de conflictos de intereses de negocio que puedan influir indebidamente en el resultado de la prueba. Además, la administración debe tomar las acciones correctivas apropiadas para hacer frente a las deficiencias encontradas como resultado de las pruebas.

6. La gerencia y el personal deben entender cómo se utilizan sus informes de BSA

Para que la gerencia comprenda la importancia del programa de ALD, es esencial que entienda el propósito de los informes requeridos por la BSA. Los informes de BSA, si bien pueden ser intensivos en recursos, son vitales para los esfuerzos de la nación para combatir toda clase de delitos financieros; por ejemplo, las amenazas planteadas por las organizaciones terroristas, naciones rebeldes, las partes que hacen proliferar armas de destrucción masiva, el narcotráfico, las organizaciones delictivas transnacionales, las tramas de fraude y corrupción en el extranjero, y las amenazas relacionadas con lo ciber. Muchas investigaciones policiales se iniciaron y/o tuvieron más apoyo por los informes de la BSA presentados por las instituciones financieras. Los informes también promueven el intercambio internacional de información entre las unidades de inteligencia financiera (UIF) en todo el mundo,

ayudando a combatir lo que es cada vez más un delito global. Dado que los esfuerzos de ALD se centran en el movimiento de fondos delictivos por medio de instituciones financieras, por esta misma razón las instituciones financieras han recibido el mandato de presentar informes que son de uso particular para hacer cumplir la ley. El hecho de saber que existen estos informes y que serán archivados por las instituciones a menudo obliga a los delincuentes a llevar a cabo sus operaciones de manera que aumenta el riesgo de detección, que también sirve a efectos de aplicación de la ley. Los informes también ayudan a identificar tendencias significativas, las relaciones y los patrones, lo que permite que la ley vea las conexiones y las tendencias que le permiten centrar sus recursos.

Sin embargo, los informes no son sólo útiles para hacer cumplir la ley; los procesos que engendran también deben servir para mitigar el

reguladores, que algunos individuos de la alta dirección que se han negado a proporcionar los recursos adecuados para un programa de ALD pueden ser considerados responsables en forma individual por violar un pilar del programa de ALD, sobre todo si los recursos negados habrían—según FinCEN—impedido o mitigado la violación.

El asesoramiento sirve para reforzar la importancia que FinCEN ha colocado en las instituciones financieras para que hagan su parte en el esfuerzo de combatir los delitos financieros. Si bien la administración no realiza el trabajo del ALD del día a día, la gerencia debe establecer el tono desde la parte superior, la creación de una cultura de cumplimiento, tanto en palabras como en acciones, lo que permitirá que la función de cumplimiento tenga éxito. Incumbe al oficial del ALD proveer liderazgo con información sobre lo que hace la función del ALD y cómo se utilizan sus informes por



riesgo de la institución. Esto incluye los riesgos planteados por los empleados, el fraude, las amenazas relacionadas con lo ciber y clientes que participan en actividad sospechosa que podría resultar en riesgo a la reputación.

Conclusión

El mensaje es claro—el ALD es una preocupación importante para todas las instituciones financieras y se espera que suministren recursos suficientes y adecuados para hacer su parte para luchar contra la delincuencia financiera. Si bien esto no es nuevo, sí le da a la alta dirección y al consejo de administración la notificación formal que no pueden disminuir gastos a medida que implementan sus programas de ALD. Como se ha señalado en otras acciones de cumplimiento, no prestarle atención a la orientación, puede utilizarse como un factor en la evaluación de una acción legal civil o criminal. Por lo tanto, se podría esperar razonablemente, teniendo en cuenta otras declaraciones de los

medio de la comunicación permanente. Al tener una sólida comprensión de lo que hace la función de ALD y lo importante que es para los esfuerzos de aplicación de la ley en combatir el lavado de dinero, la gerencia puede ayudar a establecer el tono adecuado en la parte superior que fomente una fuerte asociación entre la institución financiera y el cumplimiento de la ley. En última instancia, gran parte del trabajo para combatir la delincuencia financiera proviene de la asociación entre la función de ALD de una institución y de su dirección, la institución y la aplicación de la ley, y entre los organismos encargados de hacer cumplir la ley en todo el mundo. Se espera que cada miembro de esta asociación haga su parte. **A**

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

La Cuarta Directiva de ALD/CFT de Europa

En febrero de 2013, la Comisión Europea adoptó dos propuestas: la Cuarta Directiva de ALD y una regulación complementaria sobre la información que debe acompañar las transferencias de fondos para garantizar la trazabilidad. En el otoño de 2014 el llamado “proyecto de directiva sobre la prevención de la utilización del sistema financiero para el lavado de dinero y la financiación del terrorismo” del Parlamento Europeo y del Consejo Europeo (la Cuarta Directiva de ALD de la UE) entraron en las rondas finales de consulta y está previsto que se sancione para fin de año. Luego debe ser implementado en la legislación nacional de los Estados miembros de la UE para el año 2017.¹

Al discutir los principales cambios en comparación con la legislación anterior e internacional, y esbozar las normas y los retos del futuro en las rondas finales de la discusión, el lector podrá hacerse una idea de los desafíos que enfrentan las instituciones financieras y las empresas en el cumplimiento de los requisitos de la Cuarta Directiva de ALD de la UE.

De la Tercera Directiva de ALD de la UE a la Cuarta

La Tercera Directiva de ALD actualmente en vigor se aplica al sector financiero (entidades de crédito, entidades financieras), así como a profesionales, tales como abogados, notarios, contadores, agentes inmobiliarios, casinos y proveedores de servicios de empresa. Su

ámbito de aplicación abarca también todos los proveedores de bienes, cuando los pagos se realizan en efectivo en exceso de 15.000 euros. Todos estos destinatarios se consideran “entidades obligadas”. La Directiva les exige a estas entidades identificar y verificar la identidad de los clientes (por la diligencia debida del cliente [CDD]) y los beneficiarios efectivos, y a supervisar las transacciones financieras de los clientes. A continuación, incluye la obligación de notificar sospechas del lavado de dinero o financiación del terrorismo a las pertinentes unidades de inteligencia financiera (UIF), así como otras obligaciones que las acompañan. La Directiva también introduce requisitos y garantías adicionales (como el requisito de llevar a cabo una diligencia debida mejorada [EDD] del cliente) para situaciones de mayor riesgo.

¹ Véase la propuesta en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0045:FIN:EN:PDF>

YOUR AD HERE

Don't miss your opportunity
to reach a readership of over
25,000 AML professionals

TO ADVERTISE HERE CONTACT:

ANDREA WINTER

1.786.871.3030

AWINTER@ACAMS.ORG

ACAMS[®] | Advancing Financial
Crime Professionals
Worldwide[®]

La Directiva propuesta amplía el ámbito de aplicación del marco actual y tiene como objetivo reforzar las obligaciones en las siguientes áreas:

- En la actualidad los profesionales financieros pueden aprovechar las normas simplificadas de diligencia debida para las transacciones procedentes de zonas en la lista de terceros países “equivalentes” de los Estados miembros. La propuesta a favor de un enfoque más basado en el riesgo, con mayores esfuerzos dirigidos a los sectores de mayor riesgo, con respecto de la CDD;
- Normas sobre requisitos de identificación de la propiedad y el mantenimiento de registros beneficiosos con respecto del beneficiario final;
- Definición de las personas políticamente expuestas (PEP) ampliada para incluir tanto a las PEP nacionales así como las extranjeras, y las de las organizaciones internacionales. La regla se aplicaría a los jefes de Estados, miembros del gobierno y del parlamento, miembros del Poder Judicial y directores de empresas estatales, entre otros, como parientes cercanos;
- También se añaden delitos fiscales a la lista de delitos precedentes del lavado de dinero;
- Alcance de las reglas ampliadas a todo el sector de los juegos de azar en lugar de sólo los casinos;

El Consejo hace un llamamiento para información sobre el beneficiario final, que se mantendrá en un ‘lugar especificado’

- El umbral para desencadenar los procedimientos de ALD de los pagos en efectivo se ha reducido de 15.000 a 7.500 euros. Los legisladores dijeron que los delincuentes se están aprovechando del umbral de 15.000 euros. A los Estados miembros se les permitiría establecer umbrales aún menores;
- La cooperación entre las UIF nacionales, que analizan y difunden información sobre sospechas de lavado de dinero o financiamiento del terrorismo fortalecido;
- La potestad administrativa sancionadora de las autoridades nacionales reforzada y la cooperación entre las autoridades nacionales en los asuntos transfronterizos requeridos.

La propuesta de reglamento sustituye al Reglamento (CE) n° 1781/2006 acerca de los ordenantes que acompañan las transferencias de fondos (en lo sucesivo también conocido como el Reglamento de Transferencias de Fondos), que tiene el objetivo de mejorar la trazabilidad de los pagos. El Reglamento de Transferencias de Fondos complementa las otras medidas de ALD asegurando que la información básica sobre el ordenante de las transferencias de fondos esté disponible de inmediato para la policía y/o las autoridades fiscales para ayudarles a detectar, investigar o enjuiciar a los terroristas u otros delincuentes y para rastrear los activos de los terroristas.

La lucha por una solución de compromiso—Parlamento, Consejo y Comisión

El Parlamento Europeo se está esforzando para lograr mayor transparencia mientras que la Comisión apunta a un arreglo más flexible.

El resultado preferido del Parlamento sería un registro central público en cada país de la UE, que listaría información sobre los propietarios beneficiarios finales de una amplia gama de entidades jurídicas, incluyendo sociedades, fundaciones, fideicomisos y participaciones. El Parlamento propone que los registros estén interconectados en toda la UE y estén “a disposición del público después de identificación previa de la persona que desee acceder a la información a través de la inscripción en línea básica”. Se han adoptado disposiciones en la Directiva modificada para asegurar la privacidad de los datos y que sólo la información mínima necesaria se coloque en el registro.

Tras meses de discusiones, el Consejo Europeo adoptó un enfoque más suave, aceptando finalmente su propio ‘planteamiento general’ en junio de 2014. El Consejo no está a favor de la creación de registros públicos, o incluso de los

El Parlamento Europeo se está esforzando para lograr mayor transparencia mientras que la Comisión apunta a un arreglo más flexible

que no son públicos. En su lugar, el Consejo hace un llamamiento para información sobre el beneficiario final, que se mantendrá en un ‘lugar especificado’, como es actualmente el caso en la mayoría de países de la UE. A los agentes de incorporación, por ejemplo, a menudo se les requiere recopilar datos de propiedad beneficiaria que deben poner a disposición de las autoridades policiales y fiscales a pedido.

La propuesta de la Comisión, publicada en junio de 2014, implica un enfoque aún más flexible en cuanto a la conservación de la información sobre el beneficiario. Su enfoque requeriría el acceso irrestricto para las autoridades competentes, las UIF y, si lo permite el Estado miembro, la entidad obligada (por ejemplo, el banco). Ello, sin embargo, permite flexibilidad a los Estados miembros para que establezcan medios para asegurarlo, al tiempo que proporciona ejemplos indicativos de la forma que puede tomar un mecanismo de almacenamiento.

Más allá de esto, la Comisión insta a que los siguientes puntos se modifiquen en el proyecto original:

- Ampliación del ámbito de aplicación de la Directiva, introduciendo requisitos para un mayor número de operadores (es decir, la reducción de 15.000 a 10.000 euros como límite de pago en efectivo por la inclusión de los comerciantes de bienes, incluyendo a los proveedores de ciertos servicios de juegos de azar);
- Un requisito para medidas basadas en pruebas, y la provisión de orientación de las autoridades europeas de supervisión, en el enfoque basado en el riesgo utilizado para mejorar la identificación de riesgos;
- Normas más estrictas sobre la CDD, por lo que se requiere que las entidades obligadas como los bancos tomen medidas reforzadas donde los riesgos son mayores, y tomen medidas simplificadas donde los riesgos se demuestren menores.



Para los servicios de juegos de azar, la posición del Consejo permite a los Estados miembros introducir exenciones, pero sólo después de una evaluación de riesgos y sin permitir excepciones para los casinos y juegos de azar transfronterizos en línea. Otros Estados miembros serán informados de las exenciones concedidas. Los Estados miembros de manera similar se permitirían excepciones, bajo determinadas condiciones, para ciertos tipos de instrumentos de dinero electrónico.

Los Estados miembros pueden establecer un nivel máximo de las multas pecuniarias de no menos de 1 millón de euros, o, en el caso de las infracciones que implican crédito o entidades financieras, un nivel máximo de las sanciones de por lo menos 5 millones de euros.²

Desafíos para la diligencia debida del cliente

Lo que parece estar claro en esta etapa, sin importar el resultado final de las negociaciones, es que se enfatizará más el enfoque basado en el riesgo mejorado junto con los requisitos de varios niveles de riesgo de evaluación interconectado a nivel de país, institución y del cliente.

Las nuevas medidas propuestas, que requieren medidas basadas en pruebas para ser implementadas y complementadas con una lista

mínima de factores por desarrollar por las Autoridades Europeas de Supervisión, se encontrarán en el núcleo de los desafíos que enfrentan las instituciones al adaptar sus sistemas existentes.

Independientemente del resultado de las negociaciones, a las instituciones y organizaciones se les requerirá centrarse más en el riesgo en la forma en que administran sus programas de CDD. Esto se aplica no sólo a la cuestión de si debería aplicarse uno simplificado o EDD sino también a que si los métodos, fuentes y enfoques de monitoreo son apropiados.

Desarrollar herramientas sofisticadas y flexibles de evaluación de riesgos será esencial con el fin de generar una base más sólida sobre la que sean posibles decisiones en función del riesgo y decisión basada en la evidencia.

Conclusión

El proyecto de Directiva no sólo busca cumplir con las modificaciones introducidas por el Grupo de Acción Financiera Internacional (GAFI) en las recomendaciones revisadas publicadas en 2012, pero va más allá de los requisitos internacionales para ampliar el alcance a una mayor transparencia *vis-à-vis* la propiedad efectiva de las corporaciones, una cuestión de controversia en las discusiones de *Triologue* en curso. La revisión de la ley debe

finalizarse este otoño en las negociaciones de *Triologue* que comienzan con los auspicios de la Presidencia italiana, que finaliza en diciembre de 2014. Como se informó en el *EUobserver*, a pesar de que no será fácil llegar a un acuerdo definitivo sobre la Cuarta Directiva de ALD de la UE, todos los ingredientes para un nuevo régimen de ALD innovador están sobre la mesa.

Esas organizaciones, que ya han implementado las normas revisadas del GAFI, lo más probable es que sólo tendrán que hacer algunos pequeños ajustes a sus sistemas, incluyendo la puesta en práctica de las evaluaciones de riesgos sobre la base de los requisitos presentados por los reguladores. Esas organizaciones, cuyos procesos aún están incrustados en la Tercera Directiva ALD/CFT de la UE, se enfrentarán con las reformas más importantes, en particular en relación con el tema de las PEP. La tendencia general de la nueva Directiva ya está clara, por lo que las organizaciones pueden comenzar a planificar su viaje hacia la implementación. **A**

Jennifer Hanley-Giersch, CAMS, socia gerente, Berlin Risk Limited, Berlín, Alemania, Jennifer.hanley@berlinrisk.com

² Véase el comunicado de prensa: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ecofin/143250.pdf

ORIENTACIÓN DEL COMITÉ DE BASILEA SOBRE CÓMO GESTIONAR EL RIESGO DE LD Y FT:

PARTE II

Gestión a nivel de empresa y el papel de los supervisores en el ALD

Este es el segundo de dos artículos que abordan la orientación sobre la *Adecuada Gestión de los Riesgos Relacionados con el Blanqueo de Capitales y la Financiamiento del Terrorismo* del Comité de Supervisión Bancaria de Basilea (BCBS).¹ El artículo anterior se ocupó de la adecuada gestión de riesgo de los elementos esenciales del lavado de dinero (LD). Este artículo se centra en la gestión de riesgo de LD en una organización de grupo y transfronteriza, así como del papel de los supervisores. Mientras que el BCBS se centra en proporcionar orientación a los bancos, los principios generales se aplican a cualquier tipo de institución financiera que opera en un contexto grupal y/o transfronterizo.

ALD en un contexto grupal y transfronterizo

Reconociendo la naturaleza global creciente y la complejidad de las instituciones financieras, el BCBS indicó que, cuando un banco opera en varias jurisdicciones, el grupo debe desarrollar políticas y procedimientos para todo el grupo que se apliquen de manera coherente. Las políticas de todo el grupo deben establecer una línea de base y permitir la identificación y mitigación de riesgos para todo el grupo. En la medida de lo posible, la capacidad del grupo para obtener y revisar la información de acuerdo con sus políticas a nivel de grupo no debe verse afectada por las modificaciones a las políticas locales aplicables; debe existir un intercambio robusto de información entre las oficinas locales y las centrales.

Las operaciones locales deben asegurar que cumplen con los requisitos aplicables del país de acogida, aun cuando sean más estrictas que las políticas del grupo; como se señaló anteriormente, las normas a nivel de grupo establecen

un piso para garantizar la coherencia en todo el grupo. Si el país anfitrión no permite la correcta aplicación de estas normas, el oficial de antilavado de dinero (ALD) debe notificar a los supervisores de origen y el grupo debería considerar medidas adicionales para mitigar este riesgo, incluido el cierre de operaciones en el país de acogida. A modo de ejemplo, el BCBS reconoce que muchas jurisdicciones todavía restringen la capacidad de transmitir información de los clientes a través de las fronteras, lo que impide la capacidad de gestionar los riesgos de cumplimiento para todo el grupo. En situaciones en las que las normas del país de acogida complican o prohíben el cumplimiento de las normas mínimas del grupo, alentando a los bancos a cerrar sus operaciones en el país de acogida, el BCBS parece estar considerando animar a la institución a tratar de ser un instrumento para cambiar las leyes del país de acogida. Si esto no tiene éxito, el BCBS parece estar tomando una postura que obligaría al país anfitrión a modificar sus leyes mediante el fomento institucional de la eliminación del riesgo y el impacto resultante

para la economía. Para las jurisdicciones más recalcitrantes, este paso drástico puede ser necesario. Si bien esto es de una consecuencia aparentemente dura, sigue haciendo hincapié en la importancia de la gestión de riesgo de las instituciones financieras en vez de la rentabilidad; si una institución no es legalmente capaz de mitigar sus riesgos, debe tener en cuenta otros medios, que incluyen la eliminación de la fuente del riesgo.

Evaluación y gestión de riesgos

El banco debe tener un conocimiento profundo de todos los riesgos asociados a sus clientes en todo el grupo, ya sea individualmente o como categoría, y debe documentar y actualizar estos sobre una base regular, de acuerdo con los riesgos que plantean. Los criterios de calificación de riesgos deben aplicarse en todo el grupo; sin embargo, las políticas del grupo deben reconocer que los clientes de la misma categoría pueden plantear riesgos diferentes en diferentes jurisdicciones, como cuando una

¹ http://www.bis.org/publ/bcbs275_es.pdf

persona expuesta políticamente (PEP) es un cliente extranjero en una jurisdicción pero una interna en otra.

Del mismo modo, la diligencia debida del cliente (DDC) basada en el riesgo se debe aplicar en todo el grupo también. La segunda y tercera líneas de defensa (como se señala en el artículo anterior, en referencia al cumplimiento, así como otras funciones de control y de auditoría, respectivamente) deben evaluar el cumplimiento de las unidades de negocio de todos los aspectos de las políticas de grupo, incluyendo la capacidad de compartir información por encima de las fronteras. Muchas jurisdicciones permiten compartir información a través de las fronteras con el fin de mitigar el riesgo; sin embargo, en otras, las instituciones pueden necesitar encontrar soluciones locales donde la información no puede cruzar las fronteras.

Políticas y procedimientos de ALD consolidados

Los bancos deben entender el grado en que las leyes locales permiten la dependencia de otros bancos, particularmente los que están dentro del grupo; los bancos no deben confiar en los

introdutores que no cumplen con los requisitos de los procedimientos de ALD propios del banco. Este concepto también se aplica a las referencias en grupo, sobre todo cuando la información del cliente no puede compartirse a través de las fronteras. En general, los bancos deben obtener la información de los clientes y asegurarse de que esté disponible para la oficina central con el fin de supervisar el cumplimiento de las políticas a nivel de grupo (por ejemplo, vigilancia de su cumplimiento y el intercambio de resultados con la oficina central).

Los grupos deben aplicar sus políticas de ALD constantemente en todo el grupo, lo que permite variaciones en las necesidades locales y los riesgos presentados por los miembros individuales del grupo. Un banco debe integrar la información del cliente y de supervisión basándose en los resultados, no sólo en el cliente, sino también en los beneficiarios y los fondos involucrados; los bancos deben monitorear relaciones importantes de los clientes, los saldos y la actividad sobre una base consolidada, sea en la hoja de balance o fuera de balance, como activos bajo gestión o de forma fiduciaria, independientemente del lugar donde se llevan a cabo. Este monitoreo

centralizado debe incorporar el aporte local y centralizado de vigilancia para identificar patrones de actividad sospechosa en todo el grupo, no sólo en el nivel local o centralizado. Así, un grupo que incluye varios tipos de instituciones financieras, como la banca, corretaje de valores y seguros, debe tomar una visión holística en vez de buscar en cada entidad legal separada. Debido a que cada tipo de relación puede suponer un riesgo para el grupo en su conjunto, es importante tener en cuenta el panorama general en lugar de centrarse únicamente en los silos de negocio.

Los grupos deben tener un oficial de ALD de todo el grupo responsable de la gestión del riesgo de ALD de todo el grupo, incluyendo el establecimiento y la supervisión del cumplimiento de las políticas y la estrategia de todo el grupo; como con el oficial de nivel del banco, este oficial de todo el grupo debe tener la autoridad y los recursos suficientes para desempeñar estas responsabilidades.

Intercambio en todo el grupo

BCBS, al tiempo que reconoce la privacidad y normas de secreto bancario de diversas jurisdicciones, aboga firmemente por un enfoque



sobre toda la empresa para la gestión de riesgos. Las áreas de riesgo amuralladas para la supervisión por parte de la sede pueden causar problemas significativos para el grupo en su conjunto. De este modo, todas las operaciones locales deberían estar obligadas a proporcionar de forma proactiva la información relativa a clientes de mayor riesgo y las actividades de la oficina central y responder a las solicitudes de información de manera oportuna.

Las políticas de todo el grupo deben describir el proceso de intercambio de información, y, reconociendo la privacidad y normas de secreto bancario, las limitaciones o requisitos específicos de todo el almacenamiento de datos, la recuperación de información, el intercambio y la disposición de la información. El grupo debe evaluar los riesgos potenciales que plantean por la actividad en un solo lugar y si presenta riesgos para todo el grupo (por ejemplo, de un cliente en particular o una categoría de clientes); esto debe incluir políticas en la determinación de si otras entidades del grupo tienen relaciones para el (los) mismo(s) cliente(s) y que toman las medidas adecuadas, hasta e incluyendo las cuentas de cierre.

Las operaciones locales deben cooperar con las solicitudes de las autoridades competentes; una oficina central debe poder exigir que las oficinas locales revisen sus archivos para los partidos con los clientes sospechosos de complicidad en lavado de dinero e informar de ello. En los grupos financieros mixtos (por ejemplo, los que incorporan valores y las empresas de seguros), los diferentes riesgos que pueden estar presentes en las operaciones bancarias; las políticas a nivel de grupo deberían reflejar estas diferencias.

Como se señaló antes, si los requisitos locales crean limitaciones inmanejables en la capacidad de un grupo para compartir información, BCBS aconseja que el cierre de las operaciones sujetas a esa limitación puede ser necesario. BCBS se preocupa más por la seguridad global y la solidez de todo el grupo que con el cumplimiento de las normas que protegen a las operaciones locales y pueden proteger, en última instancia, a los delincuentes que acuden a estas operaciones locales debido a las protecciones de confidencialidad de los que se benefician. No debe permitirse que las preocupaciones de ALD en un área infecten el resto del grupo o permitir que persista en un grupo después de haber sido retirado del resto del grupo debido a la ineficacia de los medios de supervisión de grupo de manera integral. Si un grupo encuentra que una relación con el cliente lo mueve a preocuparse, las normas

de secreto locales no deben suponer un obstáculo para el grupo para mitigar con eficacia los riesgos que ha identificado.

El papel de los supervisores

BCBS, como un grupo de supervisores bancarios, establece expectativas para funciones de supervisión en la lucha contra el lavado de dinero. Se espera que los supervisores bancarios expongan las expectativas de regulación y supervisión apropiadas de ALD para los bancos que supervisan, para supervisar la aplicación por parte de los bancos y de imponer una serie de sanciones efectivas, proporcionadas y disuasorias cuando los bancos no cumplen con sus requisitos de ALD.

Los supervisores deberían adoptar un enfoque basado en el riesgo a la supervisión, que los obliga a tomar una serie de pasos. Deben desarrollar una comprensión profunda de los riesgos presentes en la competencia, el impacto potencial sobre las entidades supervisadas para comprender los riesgos inherentes que plantea a los bancos en la jurisdicción. También deben evaluar la adecuación de la evaluación de riesgos del banco basado en las evaluaciones nacionales de riesgo de la jurisdicción para evaluar lo bien que el banco entiende sus propios riesgos. Se deben evaluar los riesgos presentes en la entidad de destino supervisado y evaluar la adecuación y eficacia de los controles del banco. Por último, como parte de un enfoque basado en el riesgo, deben utilizar esta información para el alcance de la revisión y asignar los recursos adecuados en función de los riesgos identificados. BCBS reconoce que diferentes instituciones, líneas de negocio y tipos de clientes presentarán diferentes niveles de riesgo y pueden requerir conocimientos especializados. En consecuencia, los supervisores deben utilizar el perfil de riesgo de un banco para establecer una evaluación frecuente.

Los escrutinios no sólo deben evaluar si las políticas y los procedimientos cumplen con los requisitos legales/regulatorios, pero también deberían incluir pruebas de campo; también deben ser capaces de evaluar la aplicación de los requisitos de todo el grupo y locales, en particular si la operación local sigue el más alto de dos estándares (o ha documentado suficiente justificación de por qué no lo hace y cómo se mitiga el riesgo). Los supervisores del país de origen no deben enfrentar impedimentos en la verificación del cumplimiento por parte de un banco de las políticas de todo el grupo durante las inspecciones que haga in situ, incluidas las de secreto bancario y las leyes de protección de datos, siempre y cuando

cumplan con una necesidad de supervisión legítima y estén protegidas por las disposiciones de confidencialidad de supervisión. Cuando las normas del país de acogida siguen impidiendo el intercambio de información a los supervisores del país de origen y no hay alternativas aceptables, los supervisores del país de origen deberán informar a los supervisores del país de acogida que la operación local puede estar sujeta a medidas de control adicionales, entre ellas cerrar sus operaciones en el país de acogida.

Se espera que los supervisores bancarios expongan las expectativas de regulación y supervisión apropiadas de ALD para los bancos que supervisan

BCBS cree que no hay razón justificable de por qué las leyes locales deben impedir la transferencia de información de una operación local a su sede social o principal con fines de gestión de riesgos; si la ley local prohíbe compartir con “terceros”, es imprescindible que la oficina principal quede excluida de tal definición. BCBS cree firmemente que la gestión de riesgos en todo el grupo debería sobreponerse a reglas que podrían presentar riesgos significativos a las instituciones.

Guía para los supervisores de los bancos que usan una institución financiera o terceros para llevar a cabo la DDC

BCBS reconoce que en general hay tres tipos diferentes de dependencia, ya sea sobre terceros o la externalización/delegación de responsabilidades.

Los bancos pueden depender de DDC realizadas por otras instituciones financieras o empresas no financieras designadas y profesiones que están supervisadas para fines de ALD, generalmente cuando ya tienen una relación con el cliente, que abarca la identificación y verificación del cliente, el (los) beneficiario(s) y la comprensión, en su caso,

del propósito e índole prevista de la relación. Al depender de terceros, el banco debería obtener esta información pronto. Algunos países limitarán la confianza, por ejemplo, mediante la prohibición de las cadenas de la dependencia (es decir, lo que requiere la dependencia de relaciones con los clientes existentes) o no dependerán de entidades extranjeras.

Los bancos también pueden delegar sus obligaciones de DDC sobre una base contractual; sin embargo, mientras deleguen la ejecución de los aspectos de la DDC, conservan la responsabilidad por el cumplimiento de los requisitos legales; los países pueden imponer limitaciones o requisitos en torno a estos acuerdos y esperar una supervisión adecuada.

Los bancos que se basan en otra institución deben tener políticas claras sobre cuándo es aceptable depender de otra institución, incluida la forma de determinar si la dependencia es apropiada (por ejemplo, los factores a tener en cuenta), la forma de supervisar dicha dependencia, la documentación adecuada de las funciones y responsabilidades, y la supervisión de la gestión adecuada de los acuerdos de confianza (incluyendo la finalización de la relación con clientes de un tercero en que se confía o el arreglo con el tercero). Estas directrices también se aplican a los miembros de un grupo; sin embargo, esto puede ser mitigado si el grupo está sujeto a políticas eficaces a nivel de grupo.

Los bancos que delegan la responsabilidad de los aspectos de DDC deben ser conscientes de que esto crea una relación con el agente, y que el cliente está, en la medida en que interactúa con el agente, tratando con el banco. Esto puede plantear riesgos adicionales que deben ser controlados más allá de lo explicado por la dependencia (en los párrafos anteriores). La disposición debe documentarse formalmente, detallando las funciones y responsabilidades

y sobre todo la confidencialidad de la información del cliente. Los bancos deben realizar pruebas periódicas de tales acuerdos, incluida la identificación de los casos de incumplimiento y tomar las medidas apropiadas (por ejemplo, de remediación de defectos y de finalización de la relación).

Guía para los supervisores sobre la banca corresponsal

Reconociendo que la banca corresponsal es una empresa transfronteriza significativa, BCBS proporciona orientación sobre este tema. La banca corresponsal consiste en la prestación de servicios bancarios por un banco corresponsal a otro banco, el banco demandado; esto implica las operaciones de procesamiento de banco corresponsal para los clientes de la parte demandada, que pueden presentar riesgos específicos de lavado de dinero.

Los bancos que se dedican a la banca corresponsal deben realizar una evaluación de los riesgos y aplicar DDC basados en el riesgo correspondiente. Los bancos también deberían recopilar información suficiente sobre el demandado para ayudar a evaluar los riesgos, incluyendo la jurisdicción del demandado; si pertenece a un grupo (en las jurisdicciones en que operan las sucursales y filiales del grupo); información sobre la gestión y la propiedad, su reputación, las principales actividades comerciales, mercados de destino y la base de clientes (incluyendo su ubicación); el propósito de los servicios prestados a la parte demandada; las condiciones de regulación y supervisión bancaria; los controles de ALD del demandado; si los servicios van a ser utilizados en una cuenta por pagar a través de acuerdo; y si el demandado tiene sus propios respondedores que crearán relaciones especiales para el banco corresponsal.

Conclusión

Como he dicho en el artículo anterior, muchos de los conceptos contenidos en la guía BCBS no son nuevos en la industria. Sin embargo, es importante reconocer que se está proporcionando esta orientación a los supervisores bancarios para ayudarlos a desarrollar un entendimiento internacional común de lo que se espera de las instituciones financieras para mitigar el riesgo de lavado de dinero. La legislación armonizada en las distintas jurisdicciones elimina muchos de los incentivos para los lavadores de dinero en la búsqueda de las jurisdicciones más débiles y promueve un sistema financiero más fuerte y más seguro que puede identificar mejor el mal uso criminal del sistema y facilitar la detección, prevención y, finalmente, el enjuiciamiento de los delitos financieros. Los grupos necesitan tener una visión holística de los riesgos dentro de sus operaciones, en lugar de tratar de ver varios aspectos más pequeños de las relaciones por país, persona jurídica o línea de negocio. Una política de todo el grupo se aplica como una norma mínima en todos los aspectos del grupo, establece una base para un sólido programa de controles que se pueden adaptar para tener en cuenta las necesidades de cumplimiento locales. Este sistema de control requiere la capacidad de ver a través de todos los aspectos del grupo para ser eficaz; los focos aislados de visibilidad limitada son como puntos ciegos. Dado que uno no puede ver lo que está pasando allí, es difícil evaluar adecuadamente y remediar los riesgos presentes. No le hace bien a un grupo para hacer frente a un riesgo en casi todas sus operaciones; si todavía tiene riesgo absoluto, sigue siendo vulnerable.

BCBS también presenta una guía unificada para los supervisores sobre la forma de mirar el riesgo de lavado de dinero y la forma de abordarlo con un enfoque basado en el riesgo. También proporciona énfasis aún mayor sobre la necesidad de la supervisión de toda la empresa, incluyendo la provisión de ejemplos de cómo se puede lograr la vista de todo el grupo. Esta es una fuerte declaración de apoyo a la importancia de una visión integral y transparente, que triunfa sobre las reglas locales, a menudo abusadas por aquellos que tratan de evitar la transparencia. **A**

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

Los bancos que se basan en otra institución deben tener políticas claras sobre cuándo es aceptable depender de otra institución

La 13^a Conferencia Anual de ALD y Delito Financiero de ACAMS en un vistazo



La 13ª Conferencia Anual de ALD y Delito Financiero de ACAMS fue un gran éxito en muchos niveles. La conferencia se celebró en su ahora ubicación habitual el ARIA Resort & Casino en Las Vegas. La meticulosa planificación de eventos de ACAMS ofreció a los participantes un entorno excepcional para compartir experiencias, aprender de expertos de alto nivel de los sectores público y privado, y tener acceso a una amplia gama de proveedores de productos y servicios.

La asistencia fue un factor significativo en contribuir al éxito de la conferencia. La asistencia de este año batió el récord de conferencias con más de 2.000 participantes que representaban una mezcla diversa de sectores de la industria y experiencias profesionales. Las perspectivas valiosas de los diversos grupos de profesionales en la audiencia agregaron sustancia valiosa a las sesiones precedentes y eventos de contacto. Por un lado, hubo una amplia representación de los sectores de la industria de grandes a pequeñas empresas, incluidas las empresas tenedoras de bancos, bancos comunitarios, agentes de bolsa, asesores de inversión, seguros, tarjetas de crédito, los casinos, las fuerzas del orden, reguladores, auditores, abogados, consultores y proveedores, entre otros. Por otro lado, muchos de los participantes individuales tenían experiencia trabajando en varias capacidades en la industria: desde reguladores que se volvieron consultores y banqueros que se volvieron reguladores a representantes de valores con experiencia bancaria, a agentes encargados de hacer cumplir la ley, llegando a cumplir cargos bancarios. Todos los participantes aprovecharon su experiencia para hacer contribuciones apreciadas en sus nuevas funciones.

Además, en la conferencia se representaban muchas pistas específicas de la industria. Mientras que esto no es una nueva tendencia en la conferencia, la proporción de sesiones bancarias tradicionales en relación con las sesiones no bancarias ha comenzado a nivelarse. Con los años, ha habido más ofertas de sesiones adaptadas a la industria que atraen a un público más amplio. Esta tendencia es crucial, ya que fomenta un ambiente de cooperación y entendimiento entre segmentos a veces aislados. Por otra parte, un público que refleja el panorama de la industria financiera produce un diálogo amplio y más dinámico.

En general, las sesiones fueron bien planeadas en cuanto a la relevancia de los temas, la diversidad de los presentadores y sus conocimientos, el desarrollo de contenidos y la orientación de los moderadores del panel. En particular, se hizo hincapié en las ideas que se retendrían en el marco del discurso de clausura de cada sesión, lo que se convirtió en un mensaje de despedida coherente para tomar medidas.

Lo siguiente representa los puntos destacados que se retienen de varias sesiones en la conferencia:

- La industria se enfrenta a nuevos riesgos que surgen de circunstancias sin precedentes debido a desde la proliferación de moneda digital hasta el crecimiento de las empresas relacionadas con la marihuana.
- Las expectativas regulatorias son más altas que nunca. La línea de medición para evaluar la adecuación de las estructuras de gobernanza pondrá a prueba la profundidad de la participación de las empresas y la responsabilidad de su cumplimiento.
- Las acciones de aplicación están en aumento en todas las agencias reguladoras con penas más graves y casos complejos.
- La industria está tratando con un ambiente fluido donde la responsabilidad personal de los funcionarios de cumplimiento se ha convertido en una realidad.



Sesión de red



Sesión de red



Sesión general para preguntas y respuestas



El orador principal Peter T. Edge, director adjunto ejecutivo, Investigaciones de Seguridad de la Patria de ICE de los EE.UU.

Palabras sabias

Las ideas para retener subrayan la complejidad del entorno regulatorio actual y los desafíos que enfrentan los profesionales de cumplimiento. Un programa de cumplimiento exitoso establece un equilibrio entre mitigar eficazmente los riesgos y cumplir con las expectativas regulatorias. Durante el transcurso de la conferencia, los expertos ofrecieron sus puntos de vista sobre la forma de llegar a un equilibrio:

1. *Lo basado en el riesgo no es igual a ninguna acción de bajo riesgo*—Sesión: Optimización de la Gestión de Programas de Supervisión de ALD en Toda la Empresa
2. *Independientemente del enfoque, no se puede tercerizar la rendición de cuentas*—Sesión: Optimización de la Gestión de Programas de Supervisión de ALD en Toda la Empresa
3. *Use las medidas de evaluación para hacer un costo/beneficio de la mitigación del riesgo y el riesgo e incluya todos los recursos necesarios*—Sesión: Enfoque de Valores: La Gestión de un Programa Robusto de ALD de Broker-Dealer
4. *Remita a instancias superiores los problemas de actividades sospechosas de todas las áreas de cumplimiento, y no sólo de las cuestiones relacionadas con el ALD*—Sesión: Foco en Valores: Combatiendo las Tendencias Emergentes de Fraude en 2014
5. *Cuando se trata de pruebas del programa de cumplimiento, deje su ego en la entrada. Si usted está casado con su programa de cumplimiento, y no estas abierto a las críticas que pueden conducir a mejoras, esto puede ser perjudicial para su empresa*—Derek Ramm, Sesión: La Gestión de un Programa Robusto Broker-Dealer de ALD

Tal vez, los fragmentos de audio de los expertos son las mejores oportunidades de aprendizaje para los asistentes de la conferencia, ya que pueden ganar sabiduría estratégica y táctica de los líderes de la industria. Pero la sabiduría necesita ejecución, y en este día y época, la ejecución depende de la tecnología.

La tecnología fue otro tema importante en la conferencia como tema y como herramienta para mejorar la participación de la audiencia. La evolución de la complejidad y permanencia de la tecnología son factores críticos que afectan todos los puntos enumerados anteriormente como parte de las ideas que se retenían de la conferencia. Varias sesiones destacaron en repetidas ocasiones el uso de la minería de datos para gestionar el riesgo, identificar tendencias y tomar medidas. Estaba claro que el aumento de la analítica avanzada está presente a través de los sectores público y privado. En particular, el uso de los datos por los reguladores y la policía estaba marcado en los esfuerzos de cooperación entre la Red



Arriba a la izquierda y abajo: Sesión de red | Arriba a la derecha: Sesión general





Arriba: Sesión de red

Contra los Delitos Financieros (FinCEN) y el FBI, y por el aumento del número de acciones de ejecución impulsado por los esfuerzos de minería de datos de las agencias reguladoras. En cuanto al sector privado, la sala llena de expositores que proponen software progresivo fue un testimonio de la evolución de las soluciones basadas en la tecnología. La tecnología es el núcleo de la infraestructura de gestión de riesgos para todas las instituciones financieras.

De manera menos dramática, pero aún impactante, el uso de la tecnología durante la conferencia en las formas de redes sociales, registros digitales bajo demanda y sesiones interactivas contribuyó a una atmósfera atractiva. Del mismo modo, los riesgos potenciales asociados con el intercambio de información y seguridad de la información fueron evidentes en una forma no intencional tanto como la velocidad de acceso era un recordatorio de lo rápido que viaja la información y de las muchas maneras que la información y registros son compartidos.

Sin lugar a dudas, la tecnología es un arma de doble filo con retos y oportunidades para todos los segmentos de la industria financiera. No obstante, la tecnología todavía no reemplaza la necesidad de gente. El mensaje de los panelistas fue categórico: La necesidad de contar con una reserva de talento más grande de profesionales calificados de cumplimiento es una cuestión apremiante. En una industria en que una cultura de cumplimiento debe ser la norma, la demanda de profesionales de cumplimiento experimentados probablemente se encuentre en su punto más alto. La ironía, sin embargo, es que el riesgo de estar en el cumplimiento se encuentra, probablemente, en su máximo histórico también. Atraer a los candidatos adecuados para construir un equipo de cumplimiento sólido es una tarea difícil. De hecho, durante la conferencia hubo varias llamadas para adiestrar el talento de cumplimiento dentro de cada empresa. Múltiples panelistas indicaron que las instituciones pueden preferir adiestrar candidatos con diversas habilidades y convertirlos en expertos de cumplimiento de delitos financieros. Sea cual fuere el método que se utiliza para obtener el talento, la retención se convierte en un reto fundamental para todas las organizaciones.

Aunque algunos de los temas que se han descrito son características que se pueden esperar de un evento de ACAMS, este año más que nunca, hubo una sensación de encontrarse personalmente, conferida por los panelistas y participantes por igual. La intensidad de los temas y discusiones, la interacción entre el público y los presentadores y el gran número de participantes genera una energía que lleva para adelante. **FA**

M. Carolina Rivas, CAMS, directora, Engaged AML Solutions Inc., Plantation, FL, EE.UU., carolinari@engagedaml.com

Delito fiscal y presentación de informes:

¿Una convergencia?

En el artículo *Traffickers, Terrorists and Tax Criminals*,¹ publicado en el *Journal of International Banking and Financial Law* de 2013, traté de explicar los entonces novedosos aspectos de la delincuencia fiscal en Singapur, y cómo se ha añadido una nueva dimensión al régimen de contra financiación del terrorismo/antilavado de dinero (CTF/ALD) mediante la inclusión de ejemplos de personas que generan sus ingresos legítimamente, pero no pagan sus impuestos.

Este escenario surgió debido a las enmiendas a la Ley de Corrupción, Narcotráfico y Otros Delitos Graves (Confiscación de Beneficios) (CDSA), donde la evasión del impuesto sobre la renta y la evasión de los bienes y servicios de impuestos se convirtieron en delitos determinantes cuando se enumeran en la parte XII de la Segunda Lista de la CDSA. Sin embargo, como se explica en ese artículo, el concepto de un delito grave bajo la CDSA es bastante estrecho respecto a la evasión fiscal, ya que se limita a cuatro delitos diferentes bajo la Ley de Impuesto sobre la Renta (Ley IT) y la Ley de Bienes y Servicios de Impuestos (Ley de GST).

El delito grave extranjero correspondiente cometido offshore tendría que ser “el acto u omisión equivalente... si hubiera tenido lugar en Singapur, [y hubiera] constituido delito grave [en Singapur]” (es decir, el equivalente a los delitos previstos en la Ley de IT y la Ley de GST). Esto dio lugar a la preocupación de que no todos los delitos fiscales cometidos en el extranjero serían captados como delitos determinantes en Singapur debido a este requisito de la doble incriminación. Por ejemplo, como los impuestos sucesorios ya no existen en Singapur, en una situación en la que un residente del Reino Unido evita los impuestos sucesorios allí y remite fondos, que serían productos de delito en el Reino Unido según la Ley de

Productos de Delito del Reino Unido, a la cuenta bancaria de Singapur del residente, esos fondos no se consideran propiedad poseída en Singapur como resultado de una conducta delictiva bajo el régimen anterior.

¿Qué es un delito fiscal extranjero grave?

En mayo de 2014, un proyecto de ley fue presentado al Parlamento de Singapur para ampliar el alcance de los delitos extranjeros graves en relación a los impuestos. La siguiente definición fue aprobada por el Parlamento, y entró en vigor el 1 de septiembre del 2014 en conformidad con la CDSA publicada en la *Government Gazette* (Gaceta del Gobierno, en español) de Singapur el 29 de agosto del 2014:

“Por delito fiscal extranjero grave se hace referencia a un delito contra la ley nacional de un país extranjero que consiste en la realización de cualquiera de lo siguiente (según la descripción que sea) realizada deliberadamente con la intención de evadir cualquier impuesto de aquel país:

- a) La omisión de, o subestimación de o exageración de un envío hecho a efectos del impuesto sobre cualquier información que debe incluirse en la declaración;

¹ <http://www.wongpartnership.com/index.php/files/download/1234>

- b) Hacer cualquier declaración falsa o inscribirse en cualquier informe, reclamación o solicitud presentada, o cualquier documento o información solicitado, a los efectos de este impuesto;
- c) Dar cualquier respuesta falsa, ya sea verbalmente o por escrito, a cualquier pregunta o solicitud de información o pedido realizado a los efectos de este impuesto;
- d) No haber informado a la autoridad responsable de la recaudación de dicho impuesto, en la forma requerida, de cualquier información incorrecta que aparece en cualquier evaluación hecha por la autoridad, cuando se lo requiera;
- e) Preparar o mantener, o autorizar la preparación o mantenimiento, presentación de libros de cuenta falsos u otros registros, o falsificar o autorizar la falsificación de los libros de contabilidad o registros;
- f) Hacer uso de cualquier tipo de fraude, arte o artificio, o autorizar el uso de dicho fraude, arte o artificio”.²

Como afirmó el Subsecretario del Interior durante el debate parlamentario:

“La CDSA tiene actualmente el requisito de la doble incriminación, es decir, se reconoce un delito extranjero sólo si el mismo acto también constituye un delito en Singapur. Sin embargo, la aplicación estricta de la doble incriminación limita nuestra capacidad para procesar los casos de lavado de dinero que involucran la evasión de impuestos en el extranjero, donde no existe un equivalente local. Para solucionar esto, la definición modificada de un ‘delito extranjero grave’ incluirá un delito de

evasión fiscal extranjero, siempre y cuando el delito se ha tipificado como delito en la jurisdicción extranjera y se cometen intencionalmente con la intención de evadir impuestos. Estas enmiendas son coherentes con los compromisos de Singapur en virtud de tratados fiscales, y disuadirá que los dineros de impuestos ilícitos fluyan a Singapur”.³

Por lo tanto, todos los delitos fiscales en el extranjero, perpetrados con intención dolosa, con efectos a partir del 1 de septiembre del 2014, se convirtieron en un delito previo, y las instituciones financieras pueden tener que reconsiderar sus parámetros de conozca a su cliente (KYC) de apertura de cuenta y de vigilancia.

Claridad requerida

Con la eliminación de la doble incriminación (es decir, que el delito predicado debe ser un delito tanto en Singapur, así como en el país extranjero), a una institución financiera en Singapur se le hace responsable de comprender las leyes del país extranjero donde su cliente es un residente fiscal. Los residentes franceses adinerados pueden estar sujetos a impuestos basados en activos, por ejemplo, y esto es un concepto desconocido en Singapur. En esencia, las declaraciones de los clientes existentes en sus bancos que cumplen con impuestos sobre la renta y los bienes y servicios de los requisitos fiscales en sus países de origen ya no serían suficientes porque la definición de delito fiscal grave extranjero es muy amplia.

² <http://www.acams.org/wp-content/uploads/2014/10/63545164005065600014acts23.pdf>

³ http://www.mha.gov.sg/news_details.aspx?nid=MzE5OQ%3D%3D-jwhsBBqVYoQ%3D

Tampoco hay una definición general de “impuesto” en Singapur. En la Ley de IT, el impuesto se define estrictamente como “el impuesto sobre la renta impuesto por esta Ley”. ¿El término en la CDSA incluye la evasión de derechos de aduana, las contribuciones al fondo de pensiones u otras obligaciones aparentemente dispares? Aún de mayor complejidad son las cuestiones derivadas de los regímenes tributarios corporativos, donde los legisladores hablan de evitación “agresiva” de impuestos, y el impuesto de “inversiones”. En un artículo del *Financial Times* titulado *Tax Avoidance: The Irish Inversion* el autor afirma:

“Docenas de multinacionales estadounidenses han trasladado su base fiscal fuera del país para escaparle a la alta tasa de impuestos, el alcance global y los incentivos perversos de un sistema que ha animado a las empresas a construir un total de efectivo de \$1.000 atrapado en el extranjero. Sin embargo, las inversiones son cada vez más polémicas, centrando la atención en maniobras corporativas cuando los gobiernos de todo el mundo tienen la intención de tomar medidas enérgicas contra la evasión fiscal”.⁴

A fin de que las instituciones financieras proporcionen informes convincentes y significativos sobre transacciones sospechosas a las autoridades, sería necesario definir o dar dimensión al alcance de la palabra “impuesto” en la CDSA.

El ascenso de los regímenes de intercambio de información (EOI) de FATCA y OCDE

La Ley de Cumplimiento Fiscal de Cuentas Extranjeras (FATCA) fue promulgada por el Congreso de los EE.UU. en 2010, y ha sido discutida *ad infinitum* en otros artículos y trabajos académicos. En resumen, FATCA establece un proceso en el que las instituciones financieras (IF) extranjeras, por medio de la Autoridad Fiscal de Singapur (basado en el Acuerdo Modelo 1), deberán informar al Servicio de Impuestos Internos (IRS) de los EE.UU. información sobre las cuentas financieras en poder de los contribuyentes de los EE.UU., o por entidades extranjeras en las que los contribuyentes estadounidenses tienen una participación sustancial de la propiedad.

Tras la aplicación de FATCA en relación con las instituciones financieras con sede en Singapur, los detalles relativos a las cuentas que tienen los individuos de los EE.UU. en Singapur llegarán a ser transparentes al IRS para las IF extranjeras que se han registrado y obtenido un Número de Identificación Intermediario Global (GIIN). De manera similar, la Organización para la Cooperación y el Desarrollo Económico (OCDE) ha propuesto una estructura automática para la EOI entre las naciones, junto con una Norma de Información Común (CRS) para los países que adoptarán a través de acuerdos bilaterales. En el contexto de los individuos, la CRS propone que las instituciones financieras que informan ofrezcan, entre otras cosas, la siguiente información sobre las cuentas reportables relativas a personas físicas:

- En el caso de un individuo titular de cuenta y una persona denunciante, el nombre, la dirección, la(s) jurisdicción(es) de residencia, TIN(s) (números de identificación fiscal) y la fecha y lugar de nacimiento
- El número de cuenta (o equivalente funcional en ausencia de un número de cuenta)

- El saldo de la cuenta o el valor (incluyendo, en el caso de un Contrato de Valor de Efectivo de Seguro o Contrato de Anualidad, el valor en efectivo o valor de rescate) a partir del final del año natural correspondiente u otro período de información apropiado o, si la cuenta se cerró durante ese año o período, el cierre de la cuenta

Una convergencia sugerida

Es evidente desde el ascenso de los regímenes de FATCA y OCDE EOI, que la transparencia fiscal a través de las exigencias de información se hará más frecuente. Si bien el debate sigue siendo teórico para Singapur, en el contexto de la EOI, ya que no es uno de los primeros adoptadores de la CRS, la justificación para dicho proceso se pone de manifiesto. En una Declaración Conjunta de agosto de 2014 del Grupo de Adoptantes Tempranos, se dijo que, “La evasión fiscal es un problema global y requiere una solución global. Por consiguiente, celebramos el nuevo estándar en el intercambio automático de información entre las autoridades fiscales elaboradas por la OCDE (el estándar común de presentación de informes). Esto proporcionará un cambio en nuestra capacidad para ponerle freno a la evasión de impuestos”.⁵

El establecimiento de los delitos fiscales como delitos predichos y la imposición y expansión de los requisitos de declaración de impuestos puede parecer que se excluyen mutuamente. Pero en un examen más minucioso, la intención es la misma, es decir, para ponerle freno a la evasión de impuestos. Por lo tanto, se sugiere que los procesos de la criminalidad y la presentación de informes establezcan un puente para:

- Crear y mantener la compatibilidad de aplicación en relación con el ámbito de los delitos fiscales pertinentes y los medios para identificar, capturar y prevenir las actividades ilegales;
- Establecer un estándar para las instituciones financieras que no es imposible de aplicar debido al tamaño o la complejidad de la magnitud de los crímenes, o demasiado simplista para identificar, capturar y prevenir las actividades delictivas que se traten; y
- Proporcionar impulso e incentivo para la actividad de presentación de informes de cuentas de impuestos.

Las herramientas, por lo tanto, para cerrar el proceso son:

- Establecer una definición coherente del alcance de los delitos fiscales por cubrir por reportes de operaciones sospechosas y reportes de impuestos/intercambio de información; y
- Crear una disposición de salvaguarda en la CDSA, por la que una falta de presentación de un reporte de operación sospechosa relacionado con un penal tributario se mitiga por el hecho de que los detalles del cliente y/o cuenta pertinente se hayan presentado previamente ante las autoridades fiscales correspondientes.

En tales circunstancias, una plataforma se crearía para las entidades financieras y las autoridades fiscales pertinentes para que cooperen en la identificación y enjuiciamiento de los delincuentes impositivos. **TA**

Andrew Chou, socio, WongPartnership LLP, Singapur, andrew.chow@wongpartnership.com

⁴ <http://www.ft.com/cms/s/2/d9b4fd34-ca3f-11e3-8a31-00144feabdc0.html#axzz3I1rZ6TLs>

⁵ <http://www.oecd.org/tax/transparency/AEOIjointstatement.pdf>

Now **AT** Your Fingertips!



ACAMS Today always available
–Get the app now at
www2.acams.org/TheApp



ACAMS Today, the award-winning magazine dedicated to enhancing the skills and knowledge base for the financial crime prevention professional.

www.ACAMSToday.org

El evento inaugural del Capítulo de Greater Salt Lake City



El Capítulo de ACAMS de Greater Salt Lake City organizó su evento de lanzamiento, generosamente patrocinado por RDC, el 6 de noviembre del 2014. Con casi 70 profesionales de ALD presentes, el evento marcó un comienzo auspicioso para el capítulo. Puntualizado por unas sesiones de hacer contactos y presentaciones por Aaron Blankenstein de GE Capital (copresidente del capítulo), Aaron Stroud de RDC, y Karla Monterrosa-Yancey, jefa de redacción de ACAMS, el evento fue animado e informativo. La sesión de contactos fue demostrativa de la muy unida comunidad de servicios financieros que caracteriza a la mayor área de Greater Salt Lake City. Los asistentes incluían representantes de las instituciones financieras regionales y nacionales, así como un número de asistentes que representan a las entidades no bancarias que comparten un enfoque antilavado de dinero. Con un increíble inicio tal, el Capítulo de ACAMS de Greater Salt Lake City espera grandes cosas para el futuro. [A](#)



Escrito por: el consejo asesor del Capítulo de Greater Salt Lake City



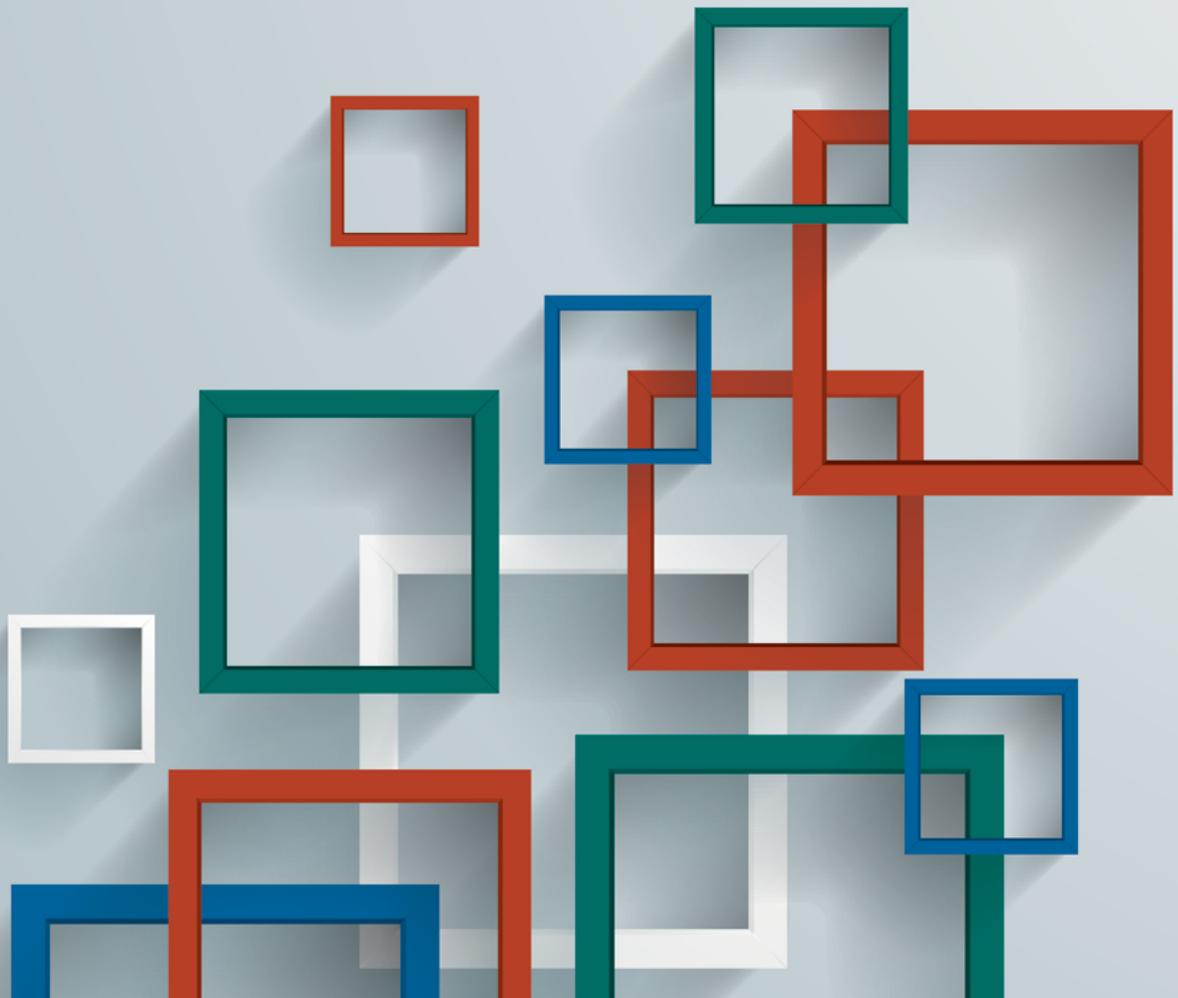
Aaron Stroud, RDC

Aaron Blankenstein, GE Capital



The stepping stone for a career in AML compliance

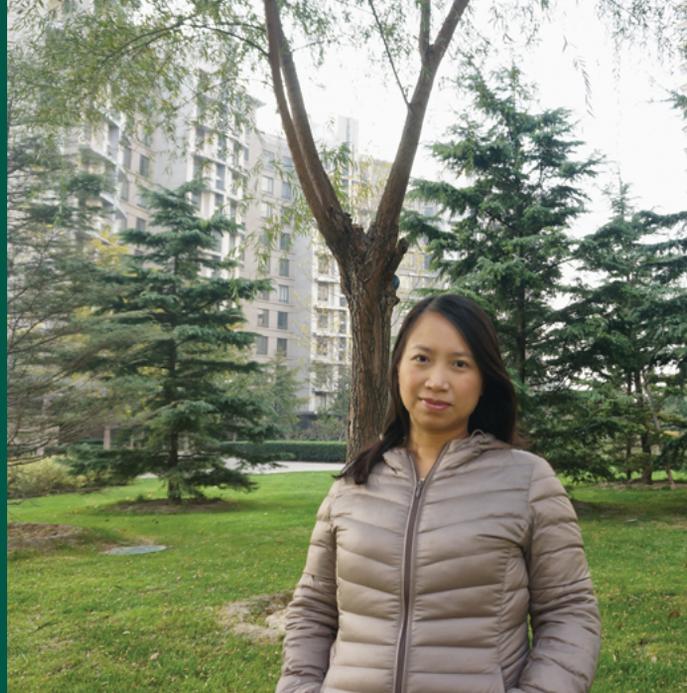
In every profession, you need that starting point – the foundation on which to build a successful career. Register for the ACAMS AML Foundations e-learning program for introductory-level AML training. Upon completion, you will have a solid understanding of AML principles and be set on the course toward earning the Certified Anti-Money Laundering Specialist (CAMS) certification.



Visit www2.acams.org/foundations for more details

Karen Yau:

La importancia de la certificación CAMS



Karen Yau se unió a la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS) en 2011. Como gerente de operaciones de la sede de ACAMS Asia, es responsable de mantener la administración y las operaciones eficientes y eficaces en la oficina de Asia, el servicio de calidad al cliente y soporte de ventas, preparación de eventos y la gestión para eventos de ACAMS y los eventos de capítulos, y otras tareas relacionadas.

Antes de unirse a ACAMS, Yau estuvo en el sector de edición y exhibición, que abarca varias industrias, durante más de 10 años. Fue jefa de ventas de publicidad de *Jewellery News Asia* en CMP Asia (luego conocido como United Business Media [UBM]), el mayor editor de la industria de joyas y organizador de exposiciones en Asia. En 2011, Hue Dang, directora de Asia de ACAMS, invitó a Yau a unirse al equipo de ACAMS.

Además, Yau tiene experiencia en ventas, gestión de ventas y en operaciones. Tiene una sólida comprensión de las necesidades del equipo de ventas y de los miembros, lo cual constituye una ventaja en su papel actual. Por otra parte, Yau ha asistido a Dang estableciendo el sistema de administración y plantillas, la mejora de la eficiencia y eficacia de las operaciones de Asia y en contratación de personal y su capacitación. También, Yau ha contribuido ampliamente a la implementación del nuevo sistema CRM de ACAMS.

Yau tiene una licenciatura en administración de empresas de la Universidad China de Hong Kong y habla inglés, mandarín y cantonés con fluidez.

ACAMS Today: ¿Cuál es la mejor parte de su trabajo?

Karen Yau: Lo que más disfruto es el establecimiento de procedimientos sistemáticos de trabajo y la búsqueda de la forma más

eficiente de resolver los problemas con el fin de atender las necesidades de colegas y clientes. La estandarización de los procesos de flujo de trabajo es esencial para nuestro funcionamiento eficiente dado que los miembros del equipo y clientes de Asia están diseminados por Asia.

AT: ¿Qué habilidades han sido cruciales para su éxito como gerente de operaciones?

KY: Para mí, ha sido tratar de todas las maneras posibles de hacer las cosas de modo eficaz—la creación de plantillas de trabajo y módulos estandarizados y útiles para el equipo son elementos clave.

AT: ¿Qué consejo les daría a los profesionales de la prevención de los delitos financieros en Asia para 2015?

KY: Habiendo estado en ACAMS por varios años, he visto el crecimiento marcado de nuevos candidatos en Asia obteniendo el certificado CAMS y asistiendo a los eventos de capacitación de ACAMS o capítulos locales. Si alguien está considerando la posibilidad de avanzar en su carrera por medio de la obtención de la calificación profesional de CAMS, cuanto antes, mejor.

AT: ¿Cuál evento de ACAMS consideraría más memorable y por qué?

KY: Mi primera Conferencia de ACAMS del Pacífico de Asia en Beijing en 2011, sería uno de mis eventos más memorables. Con el esfuerzo conjunto del equipo y de los socios, recibimos con éxito un grupo de delegados de Bangladesh dispuestos a unirse a la conferencia abordando una serie de dificultades, como falta de tiempo, solicitudes de visado, organización de viajes, etc. La participación exitosa del grupo de Bangladesh no sólo aumentó el número de asistentes de manera significativa sino también subrayó la creciente popularidad y la importancia de los acontecimientos de ACAMS en Asia.

AT: ¿Qué te gusta hacer en tu tiempo libre?

KY: Normalmente paso el tiempo con mi familia. Nos gusta visitar lugares históricos y paisajes hermosos durante los fines de semana. También me encanta leer. 

Entrevistada por:

Alexa Serrano, asistente editorial, ACAMS, Miami, FL, EE.UU., aserrano@acams.org

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



Graduados de CAMS-Audit

BARBADOS

Shonda S. Forde

BRASIL

Daniel Vieira

BERMUDA

Jay Smith

CURAÇAO

Jennifer Dors

ESTADOS UNIDOS

Susan Cannon

Tamara A. Darnow

Kacy Drury

Abdul Khan

Cheryl Sincock

Jaime A. Verastegui

PAÍSES BAJO

David G. Specker

REINO UNIDO

Bukola Adisa



Primera Fila (de izquierda a derecha): Mark Wolfrey, CAMS-Audit; Donna Davidek, CAMS-Audit; Marianne Schmitt, CAMS-Audit, CAMS-FCI; Kenneth Simmons, CAMS-Audit–Review Board Member, CAMS-Audit; Peter Wild, CAMS-Audit–Faculty and Review Board Member, CAMS-Audit; Nancy Lake, CAMS-Audit; Susan Cannon, CAMS-Audit; Kathe Dunne, CAMS-Audit.

Fila del Medio (de izquierda a derecha): Juan Carlos Ariza, CAMS-FCI; Angel Nguyen, CAMS–Faculty, CAMS-FCI; Elizabeth Slim, CAMS–Faculty and Review Board Member, CAMS-Audit; Joyce Broome, CAMS-Audit; Kata Martinez, Advanced Certification Program Administrator; Sam Adam Elnagdy, CAMS-Audit.

Fila Superior (de izquierda a derecha): Zachary Miller, CAMS-FCI; Svetlana Agayeva, CAMS-Audit; Lauren Kohr, CAMS-FCI; Brian Stoekert, CAMS–Faculty, CAMS-FCI; Chuck Taylor, CAMS–Faculty and Review Board Member, CAMS-Audit; John Byrne, Esq., CAMS–ACAMS Executive Vice President, Faculty–CAMS-Audit (and) Review Board Member–CAMS-FCI; Jonathan Estreich, CAMS-Audit; Vasilios Chrisos, CAMS–Faculty, CAMS-Audit; Brian Vitale, CAMS-Audit.



Graduados de CAMS-FCI

CANADÁ

Linda Caron

ESTADOS UNIDOS

Juan Carlos Ariza

Lauren Kohr

Latena Lee

Tom Lorenz

Scott Mauro

Zachary Miller

Kathy Ruggiero

Marianne Schmitt



Graduados de CAMS: Agosto-Octubre

Albania

Dritan Dezhgiu
Doriana Larti

Antigua y Barbuda

Either Hunte
Genisse Looby
Dorothy Peters-Nicholls

Argentina

Mirta Carrera

Aruba

Myrna Croeze
Altigracia Dania
Natalie Oosten Doorenbos
Keoma Riley

Australia

Jarrod Brugel
Brian Dovel
Mary Gamboa
Daniel Grygier
Rini Marsita
Georgia Prior
Haseeb Raza
Dylan Ryan
Chun Pong Wong

Azerbaiján

Samir Bayramov
Kamil Latifov

Bahamas

Endric Deleveaux
Nichollette Shepherd

Bahrein

Sandip Agarwal
Husain Ali
Reema Isa Al-Rabea
Shakir Shahzad Khan
Muhammad Akram Khan Lodhi
Baris Sinan Ural

Bélgica

Patricia Van Damme

Bulgaria

Kaloyan Petrov
Vesela Stefanova

Camboya

Jia Lin

Canadá

Holly Allardyce
Sarah Asals
Mark Bachrynowski
Patrick Bagstad
Jane Beaudoin
Marlieske Bloxham
Christopher Brown
Omar Bunsie
Agnes Cheung
Makaiko Chirambo
Lance Comeau
Graham Connor
Patrick Cummings
Linda Decicchio
Natalia Dobrina
Kay Dobson
Lindsay Fitzmaurice
Christiane Gzaille

Jonathan Gibeault Roy
Shaun Gossai
Mohammad Lutful Haque

Brigitte Hubert
Kamatchi Jayaraman

Zara Keryan
Alex Khosrovaneh

Brett Konyu
Demeter Kotsonis

Koffi Kouame
Yuliya Kovalchuk

Lee Hong (Clemence) Lai
Alfie Lam

Evelyn Lam
Zhihui (Mike) Lin

Adrian Lo
Ryan McKnight

Victor Mestnikov

Pavel Murakhovskiy
Edward Nagel
Declan Nicholls
David Pamentor
Leslie Pearson
Aurelio Perez
Dhanraj Persaud
Richard Porter
Marwa Ragab
Steve Rashid
Yenni Redjah
Drake Reid
Daniel Rodrigues
Duvaraga Selvaratnam
R. Brian Smallhorn
Titik Sugijoto
Susan Thomas
Misha Vlaskalin
Kellie Walsh
Lindsay Winters
Jason Woo
Yves Yao
Jeffrey Yewer
Ying Mei Zheng

Chile

Maria José Díaz Enríquez
Verónica Flottes
Estefanía Morales Lola
Arturo Muñoz Contreras
Carlos Valenzuela
Rocio Villafaña Brown

China

Wei Cai
Wenyan Cai
Jiayin Cao
Mingxin Cao
Bo Chen
Cheng Chen
Fang Chen
Fengqi Chen
Hongyu Chen
Jing Chen
Lu Chen
Yanyan Chen
Zhihua Chen
Jie Dai
Zengzhaxi Dan
Fei Ding
Rui Ding
Cen Dong
Jianmin Dou
Leilei Du
Ruoyan Fan
Jingfang Fei
Baodan Fu
Yibin Fu
Yuanyuan Fu
Hao Gao
Maggie Gao
Yan Gong
Yanhua Gu

Xiaohua Guan
Fei Guo
Yuan Guo
Chunlan Han
Ping Han
Yu Han
Daifen He
Fang He
Ivy He
Lang He
Li He
Hui Hu
Min Hu
Wei Hu
Jessica Huang
Liling Huang
Ying Huang
Fang Jia
Hongyan Jiang
Kun Jiang
Hui Jin
Bohua Li
Caiyu Li
Dan Li
Dongxu Li
Jing Li
Juan Li
Pingping Li
Qianying Li
Shujun Li
Shuling Li
Shuo Li
Wenqian Li
Xiangqiong Li
Xinge Li
Yihong Li
Yuexu Li
Yuting Li
Zheng Li
Zhiyin Li
Huiyan Liang
Tao Liang
Liyue Liao
Hong Lin
Feng Liu
Guanrong Liu
Haibin Liu
Yang Liu
Zhiyan Liu
Lu Lu
Qing Ma
Wenyi Ma
Yuwei Miao
Jie Min
Lijia Nie
Xiaowei Pang
Xiaoxia Pang
Liangzhe Peng
Xu Qin
Xiaoyan Rao
Qun Ren
Xiaoxing Sheng

Song Song
Yan Song
Lidong Sun
Philippa Symington
Qiong Tang
Yueting Tang
Caihua Wang
Fangfang Wang
Fei Wang
Fenghui Wang
Jianying Wang
Jing Wang
Jingjing Wang
Qingyun Wang
Yu Wang
Yuanyuan Wang
Lu Wu
Xiaocun Wu
Yaping Wu
Defu Xia
Li Xian
Dacheng Xiang
Wei Xie
Jing Xiong
Jing Xu
Kaiyun Xu
Taotao Xu
Xia Xu
Siwei Yan
Ziyi Yan
Liping Yang
Vinson Yang
Ying Yang
Jie Yao
Yan You
Geng Yu
Gisele Yu
Yang Yu
Yuanyuan Yu
Xin Yuan
Min Zeng
Xiaoting Zeng
Hua Zhan
Hong Zhang
Jin Zhang
Junlin Zhang
Ling Zhang
Qi Zhang
Wenfei Zhang
Xiaoxi Zhang
Yongmei Zhang
Chen Zhao
Kening Zhao
Nan Zhao
Qi Zheng
Gang Zhou
Shuling Zhou
Yun Zhou

Corea del Sur

Jong Hyun (Charles) Kim

Costa Rica

Chris Dieckmann

Curaçao

John Romer

El Salvador

Benjamin Eduardo Alas Menjivar
Luis Alonso Lémus Torres

Emiratos Árabes Unidos

Wael Al Halabi
Khalifa Saeed Al Kuwaiti
Walid Alameddine
Ahmed Galal Mohamed Eissa Aly
Sachith Amarasekara
Umair Ghani Brohi
Hassan Mohamad Chahin
Jie Fu
Farheen Mustafa Iqbal
Aftab Ahmad Mallick
Syed Masroor
Trevor Miranda
Abid Muhammad
Glenice Quadros
Laura Reid
Chioma Roseline Unah
Dawei Wen
Elena Zaharia

España

Oscar Jimenez Reyes

Estados Unidos

Vanessa Abauza
Evguenia Abramson
Chantel Acosta
Sree Rama Adusumilli
Kayla Agran
Kathleen Alexander
Chirag Amin
Alex Amponsah
Shloka Ananthanarayanan
Allison Anderson
Robyn Anderson
Richard Arcas
John Armour
Aaron Arnold-Ralph
Radhakrishnan Asari
Theresa Asbury
Carlos Ascanio
Elizabeth Attanasio
Brian Aviles
Patricia Awot
Danish Babar
Rakhi Bahadkar
Matthew Baker
Tony Ballan
Darnella Banks
Michael Barnecut
Jared Barnes
Latisha Barnes
Ryan Barnes
Manuel Barrios
Christine Barton



Clase de CAMS-FCI del noviembre de 2014

Primera Fila (de izquierda a derecha): Umberto Lucchetti; Mary Sikazwe; Nancy Lake, CAMS-Audit; Angel Nguyen (Faculty); Ed Beemer; Henry Pleau

Segunda Fila (de izquierda a derecha): Wede Okerentugba-Thompson; Brian Stoeckert (Faculty); Dennis Lormel (Faculty); Deborah Hitzeroth; Sam Adam Elnagdy; Mary Bray; Rashid El Takash; Sean McCrossan; Chris Galloway

Evan Bates
Matthew Beaven
Ebony Bell
Charles Bennett
Robin Benson
Ibrahim Besharat
Aditi Bhardwaj
Laura Blackston
Matthew Bloom
Marilyn Boada
Robert Boda
Jason Booi
Chelsea Booth
Bradley Bossenbroek
Kyle Boulton
Steven Bowler
Jennifer Bradish
Robert Brady
Geri Brown
Patrick Brown
Tira Brown
Adam Bruno
Timothy Buckley
Maryann Bullion
Mia Burgess
Michael Burkhalter
Desmond Burnett
Kelly Burton
Hung Butzer
Joseph Blake Byrd
Anne Cadenilla
Sara Cahn
Paul Camacho
Luciana Camhaji
Adrienne Carlucci
Anthony Carrea
Kevin Carroll
Zacariah Carter
Epifania Catinella
Joseph Cecil
Chak Chan
Desmond Chan
Man Chi Cheng
Julie Cho

Robert Chung
Christopher Cicero
Mihaela Ciocanu
Toni Ciprian-Matthews
John Clifton
Thomas Clifton
Rachel Cohen
Melissa Cole
Angela Coleman
John Coleman
Maria Colon
Kevin Conlon
Tracey Conniff
Justin Cook
Stephanie Cook
Steven Cooper
Nikeisha Cornwall
Oscar Cortes
Denise Cramer
Brent Crider
Kristina Crites
Blanca Marcela Cuevas
Catherine Dachenbach
Olukemi Dada
Lindsay Dastrup
Quincy De Freitas
Barbara Deighan
Brianna Deitrich
Lorna Delisser
Sharolyn Delver
Michael Denny
Hemant Desai
Clementina Desrivieres
Gurkanwal Dhanoa
Lisa Di Ienno
Madeleine Diambra
Nikolas Dignan
Kim Do
Patrick Donegan
Brian Donohue
James Doyle
Bradley Dragoon
Terry Driver
Jane Dugan

Dmitry Dukhan
Darrell Ellsworth
Matt Engelhardt
Raymond Ernst
Kevin Escott
Cindy Espinosa
Christopher Faherty
Jennifer Fanning
Kyle Farina
Colleen Farley
Jennifer Fassler
Isabela Fengler
Sean Ferguson
Jacquelyn Fisher
Michael Flower
Jack Foley
Anton Forbes
Akira Ford
Iryna Forlenza
Justin Forsmann
Connie Frank
Ellyn Frankel
Nicholas Franki
Christopher Freiermuth
Tiffany Freiger
Anthony Friel
Chong (Jenny) Fu
Edward Fuska
Manuel Galceran
Donald Gallien
William Galvin
Kimberley Garcia
Gina Gargano Castro
Yolanda Garnett
Catherine Germani
Derek Gevanter
John Gilbride
Tracy Gilmore
Philip Ginzburg
Doreen Gokhool
Gaurav Golani
John Micah Goldston
Jennifer Gomez
Patrick Gong

Robert Good
Eshai Gorshein
Amanda Graf
Virginia Green
Joseph Greenberg
Christopher Greig
Brittany Gribble
Lawrence Grill
Henry Guilbert
Feh Gwanyalla
Ryan Haag
Kevin Haddad
Katherine Haennicke
Rozhia Haghverd
Kathleen Hall
Sheila Hall
Scott Haller
Jonathan Hamblin
Christopher Hance
Katherine Hansen
Tammy Hanson
Brittany Harper
Hamad Hassan
Brent Hausfeld
Patricia Hawkinson
Justin Haws
Natalie Hayden
Chris He
Daniel Heilbron
Michelle Heinen
William Helwagen
Shaniqua Henry
Natalie Heredia
Ruth Herring
Catherine Hiatt
Cymantha Higgins
Angela Holland
Heidi Holland
Jonathan Hollis
Jason Honeycutt
Vivian Hong
Johnson Hor
Yvette Houchins
Robbin Howard

Kendra Howley
Jerson Hsieh
Asif Huda
Elena Hughes
Jason Hummel
Sarah Ippolito
Monika Iskra
Ashley Iverson
Robert Jack
Sami Jaffery
Anurag Jain
Angelia Jenkins
Xuewen Ji
Byron Johnson
Keith Johnson
Nelvin Johnson
Cory Johnsrud
Dale Jones
Eunice Jordan
Jerica Jules
Michael Juneau
Christopher Jung
Miroslava Juscakova
Randhir Kalia
Dale Kamps
Dorota Kaszuba
Clayton Kauffman
Brendan Kelly
Hassaan Khan
Mohammad Khan
Christina Kim
Wendy Kim
Alicia Kimberlin
John King
Shane Kirner
Charity Kittler
Julia Kniesche
Emily Kohler
Joann Kokorus
Bari Koss
Jessica Kowalik
Jeffrey Kraft
Minyou Kum
Ruchika Kumar

Shannon Kustra
Anne Kwon
Pedro Laborde
Andrew Labret
Jay Lampe
Karen Langston
Leonardo Lanzetta
Mark Lauria
Jane Lawrance
Marisa Leasure
Lai Ping Lee
Jason Leeper
Bryan Matthias Lemke
Ryan Lemmers
James Leon
Darci Leonhart
Melissa Lerche
Colin Lesage
Xiaolin Li
John Lieb
Jennifer Lieberman
Jason Limbaugh
Erik Linneman
Brian Lipp
Sidney Lister
Jason Liu
Xin Yang Liu
Yunhong Liu
Max Lobo
Kristin Logadottir
David Lorino
Kun Louie
Max Low
Ryan Lucia
Matthew Luebers
Kathy Mac Enulty
Amanda Macio
Natalia Macwilliam
Kevin Maffett
John Maguire
William Mahoney
Jorge Makloof
Daniel Maloney Jr.
Philip Marachilian



Clase de CAMS-Audit del noviembre de 2014

Primera Fila (de izquierda a derecha): Claudia Gonzalez; Lindsay Dastrup; Alexandra Rosi; Laura Goldzung (Faculty)

Fila del Medio (de izquierda a derecha): Peter Wild, CAMS-Audit (Faculty); Iris Smith; Jo Ann Masiello; John McCormick; Louis Napolitano; Joseph Weber; Katuna Sinyangwe; Jochen Best

Tercera Fila (de izquierda a derecha): John Byrne (Faculty); John Galjanich; Rudolf Gomez; Martin Morris; Jonathan Kay; Marion Keyes; Christopher Luangpakdy; Jason Smith; Ralph Guillou; Michael Schidlow

Christopher Mariadason
Sara Marinello
Jose Luis Marquez Rangel
Lisa Marrapodi
Steven Martin
Joseph Iii Masi
Michael Masse
Kenneth Mathieu
Brittany Matthies
Agata Maurer
Amanda Mccann
Amanda Mcclane
Jennifer Mcconnell
Adriane McCoy
Brian Mcgillin
John Mcginley
Carrie Mcgorry
Marilyn Mcgowan
Juanita Mcgrew
Allison Mcintosh
Matthew Mcintosh
Colette Mckenzie
Kathleen Mcnerney
Stephen Mcherry
Christopher Meehan
Brian Meikel
Elan Mendel
Jona Mendoza
Sean Meriwether
Marielle Messa
Samantha Michaud
Peter Milan
Anne Miller
Erica Miller
Will Miller
Lisa Minor
Manish Mishra

Paul Missaggia
Rachel Mondragon
Chad Montgomery
Gail Monxhwedey
Luke Morgan
Lorri Moriarty
Sophie Moser
Tony Moses
Connie Moyer
Venkateshwara Mudumba
Mayra Mueller
Rajeev Muppala
Sandra Murray
Silvester Muscarella
Samar Najia
Josh Nance
Wilson Nash
Gabriel Navarro
Todd Nelson
Kristi Newell
William Newenhsen
Eric Newman
Joseph Nieciecki
Jennifer Noland
Peter Nyabiosi
Timothy O'Grady
Renato Oliveira Santos
Dana Olsen
Meghan O'Meara
Carol O'Reilly
Lisa Pacheco
Lisa Padla
Sarah Parisi
Benjamin Parker
Jamie Parker
Keith Parsons
Chris Partlow

Eric Pasquito
Alpita Patel
Vasanth Pathuri
Todd Patterson
Charles Patton
Alexanders Paupe
Heather Peck
Genise Pellegrino
Michael Pepin
Laura Perkins
Stephen Perry
Colleen Petersen
Alien Phan
Thin Phung
Denise Piccolo
Russell Pierce
Antonio Plasencia
Grace Polter
Colavito Porter
Rama Krishna Prathipati
Erika Pulido
Hassan Rami
Anthony Rauco
Alejandra Rausch
Charles Reading
Jessica Reasch
Courtney Redman
Corrine Reed
Maggie Reed
Michael Renehan
Lisa Rheinhardt
Lilly Richardson
Nathan Riley
Michele Rivera
Clay Roberts
Mista Roberts
Lanita Robinson

Carlos Rocha
Jeanne Rockman
Gustavo Rodriguez
Silvia Rodriguez Romero
Melissa Ross
Sean Roughneen
George Rowan
Neil Rubin
Richard Rubio
Christianne Rush
Edward Russino
Brendan Ryan
Dana Ryan
Hannah Ryan
Kitty Ryan
Martynas Sadauskas
Genevieve Salinas Ischy
Caroline Sanchez
David Sanchez
Yahaira Sanchez
Traci Santillanes
Baha Sarana
Stephen Sarkozy
Raji Sathappan
Jessica Sattler
Gillian Savage
Sareena Sawhney
Anthony Scaturro
Clarise Schaefer
Tyler Scheeler
Nancy Schulte
Martha Scott
Angela Seaberry
Tim Semelbauer
Michael Serra
Natalia Serra
Chintal Shah

Harita Shah
Tejas Shah
Vandana Shah
Jean Paul Shaka
Ruchi Sharma
Sally A. Sheperd
Lihua Shi
Scott Shimmin
Kristi Shinn
Larinda Sigwing
Sasha Silvey
Christina Simon
Cara Simpson
Peter Singer
Deepa Singh
Jason Singh
Shilpi Sinha
Joshua Staff
Marie Smedley
Christine Smith
Cory Smith
James Smith
Shirnelle Smith
Thomas Smith
Reneé Snell
Raul Solidum
Jeevaka Somaratne
Keith Sorrell
Natalie Soto
Mark Sovey
Anna Sperling
Robert Stamos
Jennifer Stanciff
Marissa Stano
Warren Starks
Jessica Steiner Cpa
Amber Stokes

Debra Stone
Travis Studdard
Li Su
Brian Sullivan
Kimberly Sutter
Jennifer Swieczkowski
Steven Szaroleta
Kristen Takakawa
Hazel Tan
Zhi Huai Tan
Thomas Tassy
Tania Taveras
James Theard
Athrine Thomas
Paige Thomas
Carlye Thommen
Gina Thompson
John Thorpe
Gregory A. Tolson
Anthony Tomasso
Irina Toyberman
Laurie Trent
Jennifer Trinkle
Kevin Troxell
Eugene Troyansky
Philip Tu
Christopher Tyczkowski
Gregory Uren
Roman Vaccari
J. Daniel Valdes
Meghan Van Keuren
Issiah Varela
Raul Vargas
Jose Vayas Ordonez
Thomas Velez
Jithesh Viswanadh
Valerie Vought

Eric Wagner
 Andrew Waldon
 Karina Lizbeth Walker
 Kevin Walsh
 Frank Walton
 Calen Wang
 Kailin Wang
 Matthew Ward
 Pieter Wasung
 Andrew Watne
 Marlon Watson
 John Wellman
 Joshua Wenig
 Ariene West
 Denise L. White
 Jennifer N. White
 Austin Wiehe
 Michele Wilkerson
 Joshua Williams-Como
 Soyini Winnier
 Trenten Woelfel
 Chun Ting Wong
 Alicia Woo
 Daniel Wood
 Sophia Wright
 Trina Wright
 Kun Xiang
 Doug Yano
 Joyce Yee
 Carolle York
 Shane J. Young
 Steven Zakrzewski
 Joseph Zarb-Cousin
 Amy Zervas
 Donna Zheng
 Vaughn Ziegler
 Theresa Zwaska

Filipinas
 Allan Julius Azcueta
 Kathrina Chua
 Jon Lloyd Cruz
 Raquel Duroy
 Yong Liu

Finlandia
 Minna Salmivirta

Francia
 James Fisher
 Guy Lustinger
 Francois Mongin

Georgia
 Medea Torchinava

Ghana
 Samuel Akrofi

Guam
 Donnalynn Camacho

Hong Kong
 Daniel Wing Ho Chan
 Ka Man Grace Chan
 Ying Ying Sherman Chan
 Chi Hang Cheung
 Kim Yu Christina Chu

Amy Cotton
 Burnston Fan
 Ray Wai Ming Fan
 Joshua Heiliczer
 Howard Ho
 Euy Jae Hong
 Neraj Sanjay Ihalagama
 Tong Mun Jin
 Eddie Kwok
 Chi Chiu Albert Lau
 Kanny Lee
 Kwai Sheung Leung
 June Chih-Wen Liao
 Ada Man
 Becky Mok
 Ajay Mundra
 Rebecca Peckham
 Khurram Pirzada
 Mark Prothero
 Manoj Ranavaya
 Ka Ni Suen
 Abedi Syed Raza Hasan
 Christy Wing Sum Tang
 Albert Tin
 Cheery Siu Ning Tsang
 Stephanie Wang
 Elsa Wong
 Siu Fai Wong
 Yin Ting Sally Woo
 Jeff Yang

India
 Dimple Atha
 Ayyappan Baburaj
 Ajeet Batra
 Nayankumar Bhosale
 Sampada Chawan
 Anusha Gopinath
 Saurabh Jain
 Ravi Kalvakolanu
 Pratibha Kuppi
 Prashant Mishra
 Savita Nair
 Santosh Pandey
 Anil Abraham Philip
 Nagulakonda Raj Gopal
 Naveen Rajegowda
 Goldee Singhal
 Nagendra Varipilli

Indonesia
 Ishak Oesman

Irlanda
 Therese Agnew
 Nuala Mannion
 Asta Naujokaityte

Islandia
 Thurstan Felstead

Islas Caimán
 Adam Keenan
 Jose Massias
 Kasinda Rankine

Islas Vírgenes Británicas

Gwendolyn Rubaine

Italia

Larry Gurwin

Japón

Teruo Itoh
 Masakazu Kitahara
 Kunio Matsufuji
 Yoshiro Obayashi
 Akito Shimada
 Mitsuha Sonozaki
 Satoshi Takahashi
 Shizuka Urano
 Nake Xu
 Hiroko Yamamoto

Jordania

Ahmad Abu Ali
 Baha'a Aldeen Al Maqousi
 Mohammad Enad Al Shorafa
 Mohammed Al-Qarra
 Heba Al-Totani
 Ali Awartany
 Omar El Ghawi
 Mohammad Jamous
 Khaldoun Masalmeh
 Yazan Qashoh
 Bashar Qassis
 Ruba Al Saqqal
 Asaad Wafa

Katar

Medha Shiralkar
 Sona Wavde

Kazajstán

Lyazzat Amirgaliyeva

Kenia

Gregory Kapsowe
 Beatrice Toroitich

Kosovo

Rreze Jaka Nushi

Kuwait

Abdelhadi Ahmed Elkabbash
 Vinayan Mangalasseri
 Sherry Oommen

La República Checa

Natalia Stankiewicz

La República Dominicana

Jose De Pool
 Jobanny Restituyo De Rubiera

Letonia

Sandra Mielava
 Valters Murnieks

Líbano

Rola Baasiri
 Andre Bayeh
 Ziad Deek

Alice Georges Haddad

Hani Ghamra
 Ghinda Yehya Hamdar Fawaz
 Stephany Hayek
 Micheline Hejeily
 Bilal Iskandarani
 Karl Soued

Lituania

Andrejus Dzeviatnikovas
 Laura Strumylaite

Macau

Sok I. Kuan
 Yuning Su

Macedonia

Jasna Chiplakoska

Malasia

Mai Chi Ha
 Nizam Md Amin
 Tashvinder Singh Pritam Singh

Mauricio

Ajam Joomun

México

Norma Arrazola Falcon
 Margarita Chavez Ordorica
 Manuel Enriquez Ruiz
 Daniel Gonzalez Jacome
 Oscar Ibarra Gomez
 Felipe Sevilla Bejarano

Nigeria

Fola Agbele
 Bobolaji Ajao
 Usman Ademola Alli
 Joseph Anwana
 Ibrahim Bello
 Victoria Masi Iseki
 Venantius Niebemuo
 Nsan Ogar
 Donatus Ogbonnaya
 Adedunni Ayoola Ojoade
 Yemi Oyewole
 Aishah Saba
 Peter Shodipo

Nueva Zelanda

Meredith Cornelius
 Amanda Kells

Omán

Sachin Soman

Países Bajos

Leonie Dieltjes
 Marianne Ganzinga
 Daniel Geresi
 José Schülenklopper
 Henriette Maria Schut

Pakistán

Muhammad Daniyal Akram
 Salima Bhayani
 Rustam Kamaluddin
 Shafreen Pyarali

Perú

Kelly Veronica Jorge Dejo

Ana María Rodríguez Zúñiga

Polonia

Oleg Abakumov
 Bertalan Bárh
 Bozena Lapiak-Chwilkowska
 Patrycja Wroblewska

Puerto Rico

Wilhem F. Ascanio Marrero
 Delia Enid Carrasquillo Sanchez

Reino Unido

Nini Abralava
 Waseem Ahsan
 Uzair Ismail Awan
 Galajo Bah
 Andrew Baker
 Anita Balasubramaniam

Akeem Balogun
 Prince Bediako
 Severine Beroard
 William Berry
 Laura Brocklesby
 Lee Byrne
 Diana Carazo

Iwona Cohen
 Hannah Collier
 Hannah Dagger
 Wayne Eales

Andrew Franklin
 Susan Gannon
 Elizabeth Hayter
 Sarah Hopkins
 Joanne Howard
 David Hughes

Tim Jackson
 Shane Jenkinson
 Simon Jenvey
 Rafal Kaminski
 Alex Meehan
 David Mutenga

Tanatsa Nyamambi
 Wanjiku Nyandusi
 John Oridupa
 Dariusz Paleczny
 Stanislav Petrov
 John Pool
 Elena Pullin

Valentina Quadri
 Daniel Quelch
 Nadia Rahman
 Michael Shipley
 Tony Thomas
 Davide Trotta
 Holly Walker
 Penelope Wright

San Cristóbal y Nieves

Livia Bertin
 Shawna Lake
 Orin Roberts

Santa Lucía

Sylvia Auguste

Singapur

Kelvin Chow
 Mamta Dattatray Hardikar
 Ji Ting Koh
 Chin Hou Leow
 Anneng Li
 Guifang Low
 Robledo Magat
 Aarthy Rangarajan
 Anne Genevieve Rosselle
 Patricia Sanz
 Veronica See
 (Allen) Sang Wee Tan
 Swetha Venkatesh
 Elaine Yam
 Cathryn Ho Yu Mien

Sudáfrica

Eckard Conradie
 Steliana Dante
 Vanessa Fourie
 Thasneem Peerthai
 Petrus Paulus Redelinghuys

Suecia

Ulla Granath
 Mikael Karlsson
 Måns Österlund
 Hakan Svensson

Suiza

Bianca Kiss
 Adrian Riche
 Dean Rowden

Tailandia

Rashkorn Chakandang
 Huagang Cui
 Niramol Ubolsuwan

Taiwán

Shun-Yi (Joyce) Chiang
 Natalie Yuh-Ching Li
 Jen Wen Liu

Trinidad y Tobago

Marissa Allum
 Kimberly Erriah-Ali

Turquía

Nurten Ortopolat

Vietnam

Bradley Bismark
 Liu Liu

Zambia

Shadrick Banda
 Kamudambo Chirwa
 Liywalii Kanyimba
 Brian Kauzeni
 Xiantao Liu
 Mwiinga Mbozi
 Lovedale Moonga
 Imataa Mubialelwa

PEPSplus

- Over 12 Million PEP relationships and associates
- Covers international and domestic PEP's
- Discover associates and beneficial owners
- Largest data set of its kind in the market today
- Easily integrated with existing systems

